Derecho a la Protección de Datos personales en la era digital: Comparativo entre las legislaciones de EE. UU, China, España y Brasil con la de Colombia

Facultad de Derecho
Universidad Autónoma Latinoamericana

Derecho a la Protección de Datos personales en la era digital: Comparativo entre las legislaciones de EE. UU, China, España y Brasil con la de Colombia

Autores
Jonathan Duque Giraldo
Lina María Gómez Flórez

Asesora
Mayda Soraya Marín Galeano
Diciembre 2020

Facultad de Derecho
Universidad Autónoma Latinoamericana

.

Dedicatoria

A mis padres por su apoyo y guía constante a través de estos años de vida.
-Jonathan Duque Giraldo

.

RESUMEN

En el presente trabajo de investigación se propone identificar cuáles son las principales diferencias existen entre las legislaciones sobre protección de datos personales de Estados Unidos, China, España, Brasil y Colombia en relación con el almacenamiento y tratamiento de los datos personales en base de datos digitales. La herramienta usada fue la construcción y medición de indicadores con el fin de brindar información relevante sobre las diferencias existentes entre legislaciones vigentes referentes a la Protección de Datos Personales.

El estudio consta de tres etapas: en una primera etapa, se construirán categorías de análisis las cuales serán abordadas a lo largo del trabajo, dándose una definición general de cada una; en una segunda, se presentarán los indicadores construidos para la medición del nivel de protección brindado, indicándose la norma en la cual se encuentra desarrollado cada uno en cada país; y en una tercera, se presentarán los resultados, los cuales constan de la medición y comparación del nivel de protección brindado por los países escogidos, la medición se hará en una escala de suficiente (cuando el país brinda un buen nivel de protección), aceptable (cuando el nivel de protección no es bueno pero tampoco es deficiente) e insuficiente (cuando el país presenta un bajo nivel de protección).

Palabras clave: Protección de datos personales, tratamiento de datos personales, bases de datos digitales, uso de redes sociales e internet.

ABSTRACT

In this research work it is proposed to identify what are the main differences between the laws on personal data protection of the United States, China, Spain, Brazil and Colombia in relation to the storage and processing of personal data in digital databases. The tool used was the construction and measurement of indicators in order to provide relevant information on the differences between current legislation regarding the Protection of Personal Data.

The study consists of three stages: in a first stage, categories of analysis will be built which will be addressed throughout the work, giving a general definition of each one; in a second, the indicators constructed to measure the level of protection provided will be presented, indicating the standard in which each one is developed in each country; and in a third, the results will be presented, which consist of the measurement and comparison of the level of protection provided by the chosen countries, the measurement will be made on a scale of sufficient (when the country provides a good level of protection), acceptable (when the level of protection is not good but it is not deficient either) and insufficient (when the country has a low level of protection).

Keywords: Personal data protection, processing of personal data, digital data bases, use of social networks and internet

Tabla de contenido

Lista de tablas

Lista de figuras

Introducción

La sociedad ha pasado por diferentes hitos, los cuales le han permitido los avances tecnológicos que hoy conocemos, así terminando el siglo XVIII y comenzando el siglo XIX, tuvo lugar la primera revolución industrial, en la cual se pasó de una economía basada en la agricultura y el comercio, a una economía industrial y mecanizada. En la segunda revolución, la electricidad y los combustibles fósiles ayudaron al crecimiento de las fábricas y la precipitación de la división del trabajo. En la tercera, la industria hizo un proceso de formalización y de automatización a gran velocidad a partir los setentas (Oliván, 2016).

Actualmente el mundo, tras un sin número de nuevos avances tecnológicos, está viviendo un nuevo giro industrial, conocido como la "cuarta revolución industrial" o "industria 4.0", en esta el mundo físico y el digital se fusionan haciendo que no pueda separarse el uno del otro. (Gasca-hurtado, G.P.; y Machuca-villefas,L., octubre, 2019). Llevando así, a que las empresas, sin importar cuál sea su tamaño, tengan que desarrollarse desde un enfoque digital con el fin de adaptarse a este nuevo mundo. Debiendo mejorar su productividad y eficacia e impulsar sus capacidades digitales con el fin de satisfacer las nuevas necesidades de sus clientes. (Fernández & y de Lama, 2018).

Las primeras ideas sobre el internet comenzaron a surgir a finales de los años 50, siendo implementada la práctica de estas, a finales de los años 60 y a lo largo de los 70. Pero solo hasta la década de los noventa se introdujo la World Wide Web, o como es mejor conocida, "La Web". (Licklider, 2002). Cuando hablamos de la web, podemos decir que se trata de "una interface unificado para el acceso a información distribuida" a través de la red (Adell & y Bellver, 1995). Esto, junto a inventos como el teléfono o el celular, ha llevado a un cambio en la forma de comunicación humana, la cual en la era actual se encuentra regida por la inmediatez y la instantaneidad. La interacción interpersonal ha empezado a transformarse del cara a cara, a una comunicación totalmente digital (March, octubre, 2012).

La tendencia a la digitalización se ha trasladado a nuestra vida cotidiana, cada día es más común conectarse a internet para diversos fines como el educativo, el económico, informativo o solo por entretenimiento. La gama de dispositivos conectados a internet es cada vez más amplia y se extiende a objetos del uso diario. Entre los dispositivos con conexión se pueden contar los celulares, vehículos, relojes, gafas, entre muchos otros (Alcaraz, 2014).

Bajo este panorama, en el cual estamos cada vez más conectados, las redes sociales se han convertido en una forma de socializar de las personas, interactuando entre estas por este medio y compartiendo aspectos cotidianos de su vida. "En diciembre de 2011, 1200 millones de usuarios del mundo –el 82% de la población mundial conectada a internet mayor de 15 años- ingresaron a un medio social, mientras que en 2007 lo hizo tan sólo un 6%" (Van Dijck, 2016, p. 10). Lo cual demuestra el gran auge que han venido teniendo.

Estas redes utilizan la interacción de sus usuarios para recolectar datos de estos, los cuales les permiten tanto trazar como perfilar predisposiciones, hábitos y opiniones de su base de usuarios (Alaimo & y Kallinikis, 2017). Los datos recolectados por las redes sociales sobre sus usuarios

dan cabida a su uso y tratamiento inadecuado, a su recolección indebida violando derechos como el derecho a la intimidad, a su venta sin consentimiento del titular a terceros, entre muchos otros

peligros a los que se encuentran expuestos los datos personales en internet, y en especial en las redes sociales. Esto se demuestra mediante las múltiples sanciones que han sido impuestas a algunas que las páginas más grandes y reconocidas por los usuarios a nivel mundial de internet.

El año 2013 la Agencia Española de Protección de Datos (AEPD), impuso a Google tres multas de 300.000 euros por tres vulneraciones graves a los derechos de los ciudadanos, las cuales eran, guardar datos de los usuarios durante periodos de tiempo indefinidos e injustificados, no informar de manera clara que los datos se pueden usar con múltiples fines, por obstaculizar e impedir en algunos casos ejercer el derecho de acceso, rectificación, cancelación y oposición (Romero, 2013).

La compañía de análisis de datos, Cambridge Analiytica, que trabajo con la campaña del Brexit en Reino Unido y con la de Donald Trump en EE.UU, uso millones de perfiles de Facebook de votantes estadounidenses para construir un software que les permitiera predecir e influir en las elecciones (Cadwalladr & y Graham-harrison, 2018). Tras las investigaciones adelantadas por este caso, la Comisión Federal de Comercio de Estados Unidos (FTC), impuso a Facebook pagar una sanción de 5.000 millones de dólares por las malas prácticas a la hora de manejar la seguridad de los datos de sus usuarios (Redacción BBC News Mundo, 2019).

Nuestro país no es ajeno a la vulneración de los datos personales a través de los medios digitales, el 20 de mayo del año 2020, la Procuraduría llamó a un juicio disciplinario a dos generales y cinco coroneles, entre otros altos mandos del ejército nacional colombiano, quienes se encontraban adscritos a distintas brigadas de inteligencia y ciberinteligencia del ejército, por presuntos perfilamientos ilegales que se habrían llevado a cabo en contra de periodistas, abogados, defensores de derechos humanos, políticos, entre otros, por parte de las unidades militares (El Tiempo, 2020).

Es por esto que es de vital importancia en la actualidad, preguntarse por la protección de nuestros datos personales en las redes sociales, y, especialmente, sí la legislación colombiana cuenta con un nivel de protección adecuado de los mismos, con relación a los niveles de protección que ofrecen otros países.

Existen varios rankings en el mundo que miden aspectos tecnológicos de los países, cada uno brindando posiciones distintas a los países según el aspecto que se pretenda medir, entre ellos podemos encontrar el índice de disponibilidad de la red[1], el ranking sobre el ecosistema de las startup[2], y el índice de competitividad digital[3]. Este último, internacional institute for management development (2020), es liderado por Estados Unidos (puesto 1) y Singapur (puesto 2), por su parte Estonia (puesto 21), que es conocido por la prensa como “el país más digitalizado del mundo” (Cerdeira. L, 2020), queda detrás de varios países europeos como Dinamarca (puesto 3), Suecia

(puesto 4), suiza (puesto 6), entre otros. En el plano latinoamericano Chile (puesto 41) es el primero en aparecer en la lista, seguido de Brasil (puesto 51) y México (puesto 54); Colombia (puesto 61) es el sexto país latinoamericano de la lista.

Cuando se realizó una revisión de la diversidad de rankings y de los artículos de revisión del tema, se encontró que independientemente de la posición ocupada por cada país de acuerdo a sus avances tecnológicos no existe relación directa con la protección que brindan las legislaciones, ello porque el grado de protección normativo está relacionado con el desarrollo que tiene cada país respecto del derecho a la intimidad y las políticas y compromisos estatales con la protección de datos y garantías de los usuarios de internet (Ruiz y Pérez, 2016; Remolina-Angarita, 2010; Bru Cuadrada, 2007; Castillo Jiménez, 2000; Gurtubay; 1994;).

En este sentido, la pregunta orientadora del presente artículo de investigación, fue **¿**Cuáles diferencias existen entre las legislaciones sobre protección de datos personales de EE. UU, China, España, Brasil y Colombia en relación con el almacenamiento y tratamiento de los datos personales en base de datos digitales?

Para ello se planteó como objetivo general: Identificar las principales diferencias existentes entre las legislaciones sobre protección de datos personales de EE. UU, China, España y Brasil y la de Colombia en relación con el uso, almacenamiento y tratamiento de los datos personales en bases de datos digitales.

Y como objetivos específicos se dio cuenta de los siguientes:

1. Definir las categorías de análisis sobre protección de datos personales y bases de datos digitales.
2. Construir indicadores para determinar cuál de las legislaciones (EEUU, China, España, Brasil y Colombia) brinda mayor protección a los datos personales en redes sociales e internet.
3. Comparar las legislaciones sobre protección a los datos personales de acuerdo con los indicadores construidos que permita saber qué grado de protección tiene cada país sobre la protección de datos en redes sociales e internet.

Metodología

El presente trabajo de investigación tiene un enfoque cualitativo, en tanto, lo que se pretende con este es interpretar de acuerdo a las normativas de los países elegidos la utilización de diferentes figuras técnicas y jurídicas que influyen en un sistema de protección de datos. En este sentido, el alcance de este estudio es descriptivo, en el cual se conceptualizaron y se midieron cualitativamente unos indicadores (Medina, López y Díaz, 2012).

La herramienta usada para las descripciones cualitativas fue la construcción de indicadores con el propósito de brindar información relevante sobre las diferencias existentes entre legislaciones vigentes referentes a la Protección de Datos Personales contemplando el nivel de protección brindado en Colombia en relación con otros países.

Se llevó a cabo un análisis de las legislaciones de los siguientes países:

- Estados Unidos, por tratarse de un país en el cual cada estado dicta su propia legislación en la materia y dar generalmente libertad a las empresas para establecer sus estándares de protección de datos (Stranieri, S., 2019), así mismo, por ser el país del cual se origina lo que algunos llaman el "modelo estadounidense".
- China, debido a que da un enfoque particular a la protección de datos, al no tener su foco en la protección de datos del individuo, sino, que parte de premisas desde lo colectivo, así mismo por encontrarse en discusión en este país varias leyes relativas a los datos personales, siendo el marco regulatorio con mayor impacto mundial, teniendo en consideración que cuenta con el 20% de los usuarios de internet a nivel global (Aránguiz, M., 2020).
- España, porque permite tener una visión del modelo europeo, el cual ha sido adoptado por varios países latinoamericanos (ADC, 2016), teniendo como referente la normativa española, así mismo, porque la agencia española de protección de datos es pionera en el desarrollo del derecho al olvido digital (Castellano, S., 2015), el cual para está, se trata a groso modo, del derecho de las personas a solicitar la supresión de sus datos personales en los buscadores de internet (Debitoor, s.f.).
- Brasil, por tratarse de una de las pocas economías importantes del mundo que aún no tenía una legislación general de protección de datos, hasta la reciente entrada en vigor de la LGPD (Bnamericas, 2020), la cual fue inspirada en el modelo europeo, aunque guardando diferencias en temas específicos por las características propias del país (E-Health Reporter, 2020).
- Colombia, además de ser el país de los autores, resulta de interés el análisis de la legislación colombiana, debido a que tiene la ley más antigua de entre los países escogidos, por lo que cabe preguntarse por su nivel de protección en la actualidad.

En este trabajo de grado se busca establecer las diferencias fundamentales entre las legislaciones con este fin se buscó medir el nivel de protección que da cada país a los datos personales contenidos en las bases de datos digitales de las redes sociales, en relación con su recolección, uso y tratamiento para así establecer cual legislación puede tener una adecuada protección en materia legislativa y que diferencias presentan entre estas.

El instrumento metodológico empleado fue la construcción de indicadores, los cuales permitieron analizar su comportamiento en cada uno de los países elegidos, para así hacer comparaciones y mediciones cualitativas sobre cada indicador construido.

Un indicador es una herramienta investigativa que consagra información o da señales de una actividad relacionada con una información base, es decir, que al crear indicadores se está queriendo brindar información relevante y única acerca e diferentes aspectos del tema propuesto sin desbordar la temática que lo compone, lo que permite profundizar en cada ámbito, definiendo sus aspectos más importantes (Coneval, 2013). La característica principal de los indicadores cualitativos, es que su resultado se refiere a una escala de valores, pudiendo expresarse esta en términos categóricos: por ejemplo, bueno, aceptable, malo; o binarios: como un sí o un no (Dane, s.f.). En esta investigación se uso una escala de: suficiente, en caso de ofrecer una protección

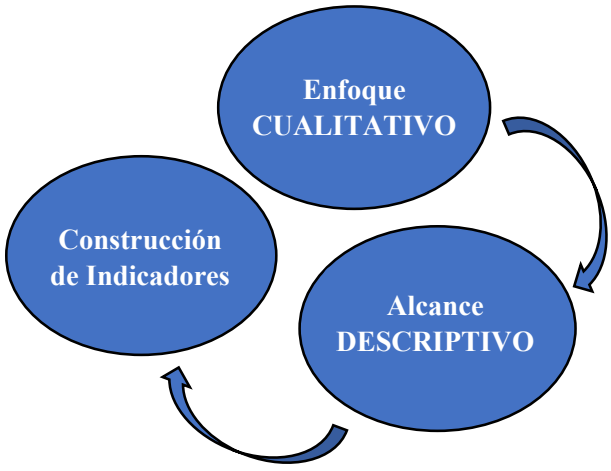
optima de los datos personales; aceptable, en caso de que su protección no sea optima, pero tampoco deficiente; e insuficiente, en caso de que su nivel de protección sea insuficiente en relación con el indicador y los demás países y modelos.

Los indicadores se diseñan a partir de factores relevantes, los cuales deben ser definidos antes de su construcción. Siendo así que, son varios los posibles indicadores que se pueden construir para cumplir con el objetivo, por lo que será el investigador quien decida que indicadores le aportan la información más útil para lo que pretende realizar (Coneval, 2013).

La importancia del manejo de indicadores o medidores es que reducen la complejidad de un tema en bloque, es decir, que simplifica la información de las múltiples perspectivas que puede tener un tema central y complejo (Schuschny, S. y Soto, H., 2009).

La técnica que se empleará para esta investigación será la revisión documental, el análisis de normas y textos respecto a la idoneidad de la normatividad en materia de protección de datos personales en la recolección, tratamiento y almacenamiento de los mismos, centrándose principalmente en la norma que regula de manera general la materia. Se usarán fuentes documentales para la realización de la investigación, siendo el campo de recolección de la información las bibliotecas, librerías, internet, noticias verídicas y otros trabajos de investigación. Esta información será registrada en fichas (resúmenes, conceptos, gráficos).

Ilustración 1. Gráfico de manejo de la metodología



Fuente: Elaboración propia de los autores.

Capítulo I. Categorías de análisis sobre protección y tratamiento de datos personales

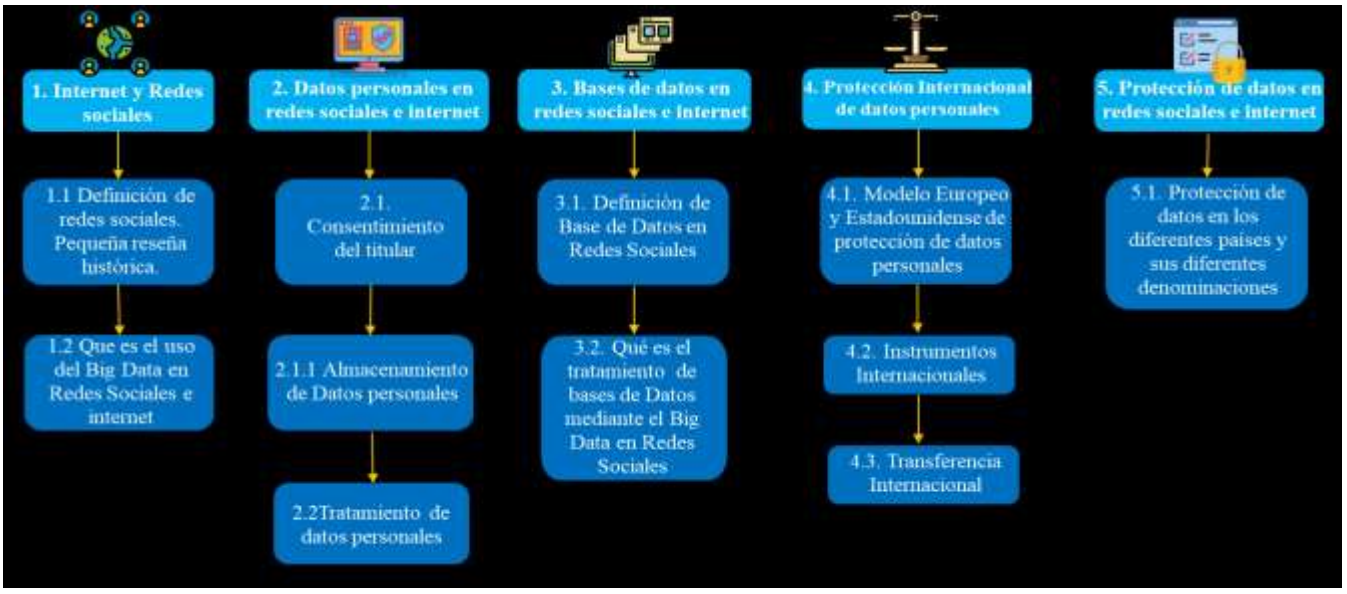
En el presente capítulo se abordarán las categorías de análisis que se desarrollarán a lo largo del trabajo, haciendo una definición básica de los conceptos que componen las mismas. Dichas categorías y sus respectivos conceptos se trabajarán desde sus definiciones básicas, sin entrar en mayores consideraciones técnicas, que serían propias de las ciencias de la computación y desbordarían el objeto de la presente investigación.

Inicialmente se dará una definición general de redes sociales y se hará una breve reseña histórica del desarrollo de las mismas. Posteriormente, se definirán algunos procesos por los que atraviesan los datos personales en las redes sociales, para llegar a dárseles un tratamiento.

Se definirá lo que son las bases de datos en redes sociales y el tratamiento que mediante el Big Data se puede hacer de la información contenida en estas. Posteriormente se indicarán los dos principales modelos de protección de datos en el mundo, y, algunos de los instrumentos internacionales expedidos en relación con la protección de datos personales y la transferencia internacional de los mismos, y, por último, se realizará un recorrido por las legislaciones de China, EE. UU, Brasil, España y Colombia, con el fin de conocer la manera como protegen los datos personales de sus ciudadanos, y la denominación que dicha protección ha adoptado en cada uno de estas.

El siguiente cuadro resume de manera general el contenido del presente capítulo:

Ilustración 2, Estructura Categorías de análisis sobre protección y tratamiento de datos personales



Fuente: Elaboración propia de los autores.

1. Internet y Redes Sociales

1.1. Redes sociales

El termino redes sociales, es un término que se suele usar cotidianamente, muchas veces sin saber realmente lo que el significado de este abarca y el impacto que ha tenido su uso en la modificación de la forma como nos relacionamos socialmente.

.

El Instituto Nacional de Tecnologías de la Comunicación de la Agencia Española de Protección de Datos (2009), realizó un estudio en el cual rastrea el origen de las redes sociales, en el año 1995, con el sitio web "classmates.com" creado para recuperar y mantener las relaciones con antiguos compañeros de clases. Otra página web ligada al surgimiento de las redes sociales, fue la página inaugurada en 1997, SixDegress.com, la cual permitía la creación de perfiles, listados de amigos, el envío de mensajes entre amigos y la navegación en la lista de amigos por parte de terceros, siendo esta última función incorporada en 1998, convirtiéndose en una novedad para en su momento (Ros-Martín, 2009).

Durante los años siguientes, especialmente después del año 2000, se vio un gran auge en la creación y expansión de redes sociales en el internet, surgiendo bajo diversas denominaciones y formas de conectar a sus usuarios a través del mundo (Ros-Martín, 2009). Siendo "la Web 2.0", que empezó a funcionar en el año 2004, un impulso para su aumento y consolidación, ayudando a dar paso así a una generación digital (de salas Nestares, 2012), la cual está cada vez más conectada e incorpora más los elementos digitales a su cotidianidad.

La creación de redes como Yahoo en la época de los 90 ayudó al surgimiento de las redes sociales. Siendo a partir del año 2003 cuando se empiezan a crear plataformas sociales cada vez más demandas por los usuarios como LinkedIn, MySpace, Hi5 y más adelante después del año 2004, la creación de aplicaciones como Facebook, YouTube, Twitter, que han generado una mayor interacción e impacto en el mundo por su cantidad de usuarios. Sin dejar de mencionar las nuevas aplicaciones que se han creado por el uso diario del móvil como lo es el WhatsApp. Hoy en día la comunicación es más inmediata tanto en el ámbito personal como el laboral (Antevio, 2016).

Desde su surgimiento, las redes sociales han ido tomando cada vez más relevancia en la vida cotidiana de las personas, convirtiéndose en un medio indispensable para la comunicación de muchas de estas, a lo largo de su historia son múltiples las definiciones que se han dado de estas y variados los autores que las han tratado de definir.

Una de estas definiciones la da el Instituto Nacional de Tecnologías de la Comunicación y la Agencia Española de Protección de Datos (2009), así:

> "Las redes sociales online son servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de los usuarios afines o no al perfil publicado" (p. 7).

Otra definición es aquella según la cual, las redes sociales son espacios donde las personas publican y comparten información tanto personal como profesional, con personas conocidas al igual que con completos desconocidos (Celaya, 2008).

Es así, como tomando las ideas de los autores anteriormente citados, podemos definir las redes sociales como sitios en internet, en los cuales las personas publican información, compartiéndola con terceros e interactuando con estos a través de estas páginas web.

Estas redes permiten compartir información e interactuar con usuarios de todo el mundo, simplemente completando un registro que permite crear un perfil en la página web y así acceder a los servicios que esta presta. Las redes sociales tanto digitales, como aquellas que no hacen parte de este ámbito, cuentan con algunas características estructurales básicas, las cuales les son generales, algunas de estas características son:

1. Tamaño: Número de personas que componen la red social.
2. Composición: Número de diferentes tipos de personas en la red.
3. Densidad: Grado de interconexión entre los miembros de la red.
4. Dispersión: Niveles de relación en términos de tiempo y espacio (Quesada, 1993).

Por su parte, los investigadores Boyd y Ellison han dado otra definición de las características compositivas de las redes sociales:

> "servicios con sede en la red que permiten a los individuos: 1) construir un perfil público o semipúblico dentro un sistema delimitado, 2) articular una lista de otros usuarios con los que comparten relaciones, 3) ver y recorrer la lista de relaciones que esas personas relacionadas tienen con otras dentro del sistema" (Boyd y Ellison, 2007, citado por Flores, Morán, Rodríguez, 2010).

Es así como las redes sociales han surgido y han aportado a la nueva era digital cambios enormes en la comunicación y en el estilo de vida de las personas. Aunque surgiendo a su par una gran cantidad peligros para los datos personales de las personales, especialmente con la implementación de nuevas herramientas para el tratamiento de grandes cantidades de datos como lo es el "Big Data".

1.2. El Uso del Big Data en Redes Sociales e Internet

Big Data y redes sociales

El gran cumulo de información que se está generando cada día en internet, especialmente en las redes sociales, ha dado lugar a una nueva tendencia, como lo es el uso del Big Data para el análisis de esta información. Cada día aplicaciones y páginas web de redes sociales como Facebook, Twitter, Whatsapp, Youtube, entre otras., reciben la visita de millones de usuarios que constantemente están interactuando con la red, generando en este proceso grandes volúmenes de

información que las empresas buscan capturar, almacenar y posteriormente analizar (Joyanes Aguilar, L., 2013).

Son múltiples los autores que han intentado dar una definición al Big Data, existiendo por ende múltiples definiciones y no una sola aceptada de manera general tanto por el sector académico como por el tecnológico. Una de estas definiciones alude a que el término Big Data hace referencia a la enorme cantidad de información contenido en bases de datos y que se someten a vastos análisis mediante algoritmos (Gil, E., 2016). Otra definición de Big Data se puede encontrar en la dada por Enrique Dans (2011) al decir que por este se entiende el "tratamiento y análisis de enormes repositorios de datos, tan desproporcionadamente grandes que resulta imposible tratarlos con las herramientas de bases de datos y analíticas convencionales" (p.1).

Esta expansión del internet, y con este, de la gran cantidad de datos que dejamos al navegar por la red, no ha pasado desapercibido para las grandes compañías tecnológicas que ven en el Big Data una gran oportunidad para aprovechar los datos que dejan los usuarios al interactuar con sus aplicaciones, buscando con esto entender mejor sus preferencias para personalizar el contenido que les envían.

Las compañías de internet se han visto particularmente abrumadas. Google procesa más de 24 petabytes al día, un volumen que representa miles de veces la totalidad del material impreso que guarda la Biblioteca del Congreso de Estados Unidos. A Facebook, una empresa que no existía hace una década, se suben más de diez millones de fotos nuevas cada hora. Sus usuarios hacen clic en el botón de "me gusta" o insertan un comentario casi tres mil millones de veces diarias, dejando un rastro digital que la compañía explota para descubrir sus preferencias (Mayer, V. y Cukier, K., 2013).

De esta manera, las compañías de redes sociales pueden utilizar las interacciones de sus usuarios para recolectar datos que les ayude a comprender mejor los gustos de estos, información que luego puede ser analizada y utilizada para crear campañas publicitarias personalizadas.

El uso del Big Data también conlleva ciertos riesgos para los titulares de los datos, entre estos podemos encontrar la creación de perfiles que no necesariamente son siempre exactos y con información verídica, suplantación de identidad, e incluso, como ya ha pasado en varios países del mundo, su uso ilegal para la obtención de fines políticos, entre muchos otros tantos peligros que puede acarrear el uso indebido de esta herramienta (Martínez Devia, A., 2019).

Uno de estos riesgos se materializó en la campaña presidencial estadounidense del año 2016, en la cual la empresa Cambridge Analytica recopiló la información de millones de usuarios de Facebook, sin contar con el consentimiento de sus titulares, información que fue utilizada en beneficio de la campaña de Donald Trump. Esta misma empresa se encuentra enfrentando investigaciones en Reino Unido por presuntamente haber influido, mediante actividades ilegales, en la campaña del brexit (Rosenberg, M., Confessore, N., y Cadwalladr, C., 2018).

Esto demuestra los peligros a los que se encuentran expuestos los datos personales de las personas al hacer uso de las redes sociales en internet, debido al tratamiento indebido al que estos pueden

ser sometidos, tratamiento que puede tener como fin, desde el éxito de la campaña publicitaria de una empresa, hasta el éxito de la campaña electoral de un político. Es por esta razón, que en un mundo tan interconectado y dependiente de la tecnología como en el que actualmente vivimos, la protección de los datos personales en internet y especialmente en las redes sociales -debido al tipo de datos que en estas se maneja-, se debe convertir en uno de los puntos centrales de debate de la agenda legislativa de los países.

2. Datos Personales en Redes Sociales e Internet

Se entiende como dato personal toda información básica que cuente con la capacidad de llevar a la identificación de una determinada persona física identificada o identificable, contenidos o almacenados en diferentes bases de datos, tales como, bases de datos públicas o privadas de información financiera, crediticia, comercial y hasta en el uso constante de herramientas personales como los smartphones y las computadoras. Esto sin perjuicio de la anonimación del dato objeto de manipulación (Comisión Europea, s.f.).

Otra de las definiciones que se puede dar de datos personales, recogida de múltiples ordenamientos internacionales, dice que se concibe como tal "cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados" (Anguiano, J. A. H., 2020).

2.1. Consentimiento del Titular

El consentimiento informado del titular de los datos personales sometidos a tratamiento es un componente importante para el tratamiento de los datos personales, este consentimiento debe ser previo a la recolección y tratamiento, inequívoco e informado para que se garantice una expresión del consentimiento que se encuentre exenta de vicios, sin este no es posible en ningún caso que se someta la información a manipulación alguna. Por otra parte, un elemento que reviste el consentimiento del titular, para el tratamiento de datos personales, es la ‘’necesidad’’, esta última hace referencia a que para que se pueda llevar a cabo el tratamiento de datos por parte del operador, debe existir una razón lícita y necesaria para el fin que se busca obtener, para poder hacer el uso de estos, pues sin todos los requisitos para la manipulación, no ha de existir un consentimiento válido que permita un uso adecuado y respetuoso de los derechos. (Gil, E., 2016).

Para obtener un consentimiento libre de vicios, es necesario que el mismo abarque algunos requisitos, sin los cuales, como se dijo anteriormente, no podríamos hablar de un consentimiento válido. Tales requisitos son: contar con el consentimiento libre del titular de los datos, sin que en este hayan mediado inferencias externas; inequívoco, que permita apreciar la voluntad del titular; expreso, que lo haya manifestado por algún medio; específico, que no es más que, el conocimiento de cuál es el fin del uso y el tratamiento de los datos que se llevará a cabo; y, finalmente, que el consentimiento sea informado, que haya total transparencia para con el titular de los datos a tratar (Trujillo Cabrera, 2018).

2.1.1. Almacenamiento De Datos

El almacenamiento de datos consiste en la creación y manejo de sistemas de almacenamiento que permita contar con la capacidad de espacio en los discos duros que se requiere hoy en día para almacenar datos de manera eficiente. Sistemas de almacenamiento masivo como lo son: DAS, NAS, SAN y sistemas de almacenamiento en la nube que permiten la administración exitosa de los datos personales. Es a partir del siglo XX cuando se empieza a ver lo que es el almacenamiento de datos tal como lo conocemos hoy en día, con la creación de las computadoras electrónicas, habiendo hoy infinidades los sistemas de almacenamiento que existen en todos los dispositivos electrónicos y de internet en el mundo. Desde hace varios siglos ha ido surgiendo la necesidad de crear diferentes sistemas de almacenamiento de datos, pues las cantidades que se crean a diario es mayor a las opciones de almacenamiento que existen, es más fácil producir datos que tener el control y la capacidad de almacenarlos; en un año es posible que se generen hasta 5 Exabytes de información, la cual tiende a crecer a medida que evoluciona la tecnología (Vázquez, S., 2015).

Otra definición sobre lo que consiste el almacenamiento de datos, es la señalada por Arévalo, (2017):

> '' El almacenamiento es una de las actividades o capacidades más importantes, ya que a través de ésta el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos'' (p.10).

Es así entonces, como este concepto ha venido tomando forma desde hace varios años generando a la industria tecnológica grandes retos para evolucionar y reinventarse, haciendo la navegación en internet más eficaz y fácil para el ser humano, dejando a su paso otras necesidades, como lo es hoy la protección los datos personales de los usuarios, que estos dejan al navegar en internet.

2.2. Tratamiento de datos

El tratamiento de datos se puede definir como "cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Aika Soluciones, 2016, p. 5)".

Entiéndase por tal la actuación, manipulación o maniobra que, relacionada con el dato de una persona, permita su individualización física como tal, cuyo tratamiento esté sometido a procedimientos manuales o automatizados requeridos desde el momento de la recolección del dato para un fin determinado (Comisión Europea).

El tratamiento de datos en las redes sociales comienza a llevarse a cabo a partir del mismo momento en que se crea la red social, donde los usuarios terminan compartiendo datos íntimos que permiten saber más sobre la persona. De este modo el proveedor de la red social comienza a hacer recolección y tratamiento de los datos, cuando son depositados (Hellasconsultores, 2013).

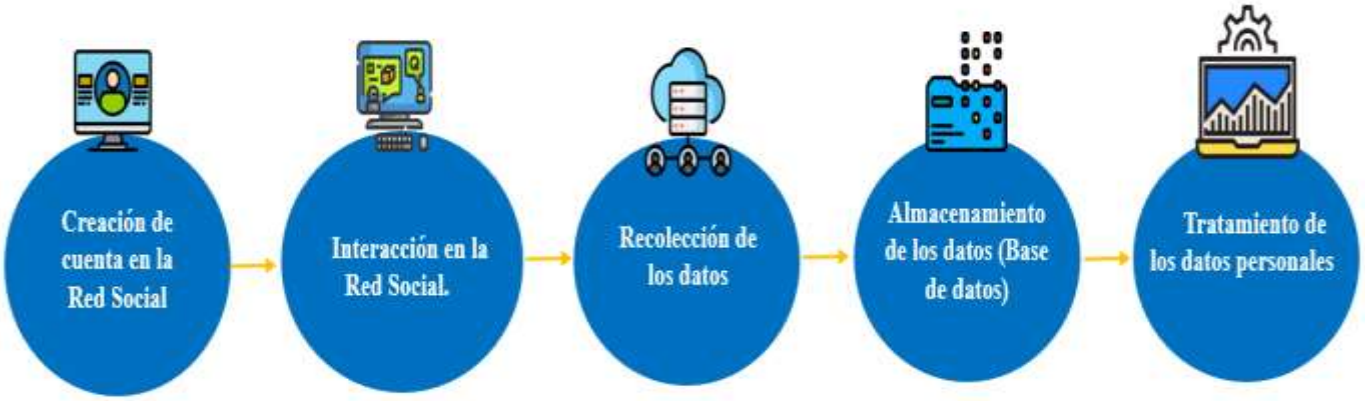
Una finalidad del tratamiento de datos es lograr ofrecer a una organización o a cualquier persona un sistema eficiente que permita la gestión de información para adquirir, transmitir y producir datos al menor costo económico y que la información sea la más actualizada, exacta y clara posible

para que tal actividad sea exitosa para lograr influenciar en la toma de diversas decisiones (Arevalo, J., 2017).

Así mismo, hay algunas características que conlleva el tratamiento de datos que permite un mejor abarcamiento del concepto, al respecto Arévalo (2017), señala lo siguiente:

> ‘’El Sistema de Gestión de Información es el encargado de seleccionar, procesar y distribuir la información procedente de los ámbitos interno, externo y corporativo. • Información interna. La producida en la actividad cotidiana de la institución • Información externa. La adquirida por la institución para disponer de información sobre los temas de su interés • Información corporativa o pública. La que la institución emite al exterior.’’ (p.9).

Ilustración 3 Tratamiento de datos personales



Fuente: Elaboración propia de los autores.

Se muestra una representación gráfica del proceso que atraviesan los datos personales, desde el momento en que estos son generados, hasta llegar a su posterior tratamiento. La representación plasmada en el gráfico se trata de una representación básica, sin entrar en consideraciones técnicas propias de las ciencias de la computación, las cuales implicarían un análisis más profundo de cada una de sus etapas, teniendo en consideración las múltiples herramientas que en cada una de estas entran en juego. Dichas consideraciones técnicas desbordarían el objeto del presente trabajo, por lo cual, solo se trabajarán aquellos aspectos básicos que sean útiles para el desarrollo de la presente investigación.

3. Bases de Datos en Redes Sociales e Internet

3.1. Definición de Base de Datos en Redes Sociales

El mundo está constantemente evolucionando, en el siglo XXI es cada vez mayor el número de herramientas tecnológicas inventadas, las cuales han llevado al ser humano a estar cada vez más conectado a internet, entre estas se cuentan relojes inteligentes, televisores inteligentes, carros inteligentes, entre un sin número de nuevas invenciones que han logrado conectar a la red elementos de uso cotidiano que antes no lo estaban.

El uso diario de estas herramientas deja a su paso un gran volumen de datos, producto del uso y manejo diario de las mismas; estos datos son recolectados y almacenados, dando cabida a que los mismos sean sometidos a diferentes análisis con el fin de obtener algunos resultados como las preferencias e intereses de las personas, toma de decisiones, reconocimiento de voz, situación económica, salud, ubicación entre otros aspectos de la vida personal y cotidiana de una persona. Son resultados que salen de la sistematización de algoritmos que permiten la extracción de aquella información que se busca, y que nos muestra un nuevo fenómeno de la tecnología, que hoy es conocido como Big Data, permitiendo convertir en información aspectos de la vida cotidiana (Martínez Devia, 2019).

El almacenamiento de estos datos recolectados sea por parte del sector público o del privado, se realiza mediante las bases de datos con que estas cuentan.

Son diversas las definiciones que de bases de datos se ha dado a lo largo de su historia, cambiando estas según el tipo de base de datos de que se trate, pero algunos autores han logrado definirlas de manera general. Una de estas definiciones es la siguiente:

> "Una base de datos es un conjunto de información relacionada que pertenece a una organización y que está agrupada como un todo. En la base de datos de una juguetería, por ejemplo, estará reunida la información de los juguetes (precio, cantidad en stock), así como los datos de los proveedores (dirección, teléfono, saldo deudor), clientes (si se desea llevar información individualizada de cada uno de ellos), empleados (salarios, presentismo, comisiones de los vendedores), contabilidad (cobranzas, pagos, liquidaciones), etc" (Frassia, Mercedes, p. 9).

Otra definición general que se puede encontrar de bases de datos es:

> "Una base de datos es un conjunto de datos almacenados en memoria externa que están organizados mediante una estructura de datos. Cada base de datos ha sido diseñada para satisfacer los requisitos de información de una empresa u otro tipo de organización, como, por ejemplo, una universidad o un hospital" (Marqués Andrés, 2011, p. 10).

Así es que, las bases de datos de las redes sociales, son aquellas en las que se contiene un conjunto de datos organizados bajo determinada estructura, recolectados por parte de la compañía prestadora del servicio, de las interacciones y publicaciones de los usuarios de estas, en su sitio web o aplicaciones móviles.

3.2.Tratamiento de bases de datos mediante el Big Data en redes sociales

A su vez, compañías externas pueden crear bases de datos propias a través del análisis de las bases de datos de distintas redes sociales, acumulando datos sobre el usuario que les permite clasificarlos en ciertas categorías en base con la información que sobre este se ha recabado. Tal es el caso de la compañía tecnológica, AT&T Inc, la cual cuenta con una patente, a través de su sociedad AT&T Intellectual Property I, L.P., que analiza una pluralidad de redes sociales, analizando los sentimientos del usuario para categorizarlo por ciertos temas, guardando los resultados para posteriormente influenciar en su forma de ver un producto, buscando que esta sea más favorable (Estados Unidos Patente nº US9262517B2, 2010).

Muchas de estas empresas, dedicadas al análisis de datos, deben hacer uso del big data debido a que, gracias al gran flujo de información que producen los usuarios de las redes sociales mediante la interacción con la plataforma de la red, los equipos tradicionales se han vuelto obsoletos a la hora de analizarla, por lo que han encontrado en el big data y su capacidad de analizar grandes volúmenes de datos en tiempo real, una solución. Los pioneros en la explotación de esta información son tanto grandes compañías tecnológicas como Amazon, Netflix y Google; como redes sociales, tales como, Twitter, Snapchat, Instagram o Facebook, las cuales la almacenan en sus bases de datos, para con esta construir perfiles de sus usuarios, con fines principalmente publicitarios (Gonzalez, 2019).

4. Protección internacional de datos personales

4.1. Modelo europeo y estadounidense de protección de datos personales.

Se habla de dos vertientes o modelos de protección de datos a nivel mundial, el modelo europeo y el estadounidense. El modelo europeo tiene normas de aplicación general con desarrollo en sectores específicos, mientras que, en el modelo estadounidense, no se cuenta con una ley federal general sino con múltiples normas en sectores específicos, así como regulaciones propias de cada estado (Davara. I, 2017). La motivación del modelo europeo son los derechos humanos del individuo, mientras que el modelo estadounidense surge de motivos principalmente empresariales (Pérez. G y González. I, 2012).

4.2. Instrumentos internacionales relativos a la protección de datos personales

La definición de ciertas normativas para la protección de datos personales, ya no es un asunto meramente local que atañe solo a cada Estado, sino que, ahora más que nunca, debido al flujo transnacional de estos generado por su comercialización entre estados y de un mundo globalizado, este asunto trasciende hasta la esfera internacional (Valbuena Abogados, 2017).

Inicialmente los instrumentos internacionales no hacían mención expresa al derecho a la protección de datos personales, sino que el mismo era protegido mediante el derecho a la vida privada, debido a que ambos se encuentran estrechamente ligados. Entre estos instrumentos internacionales podemos encontrar la Declaración Universal de los Derechos Humanos de 1948 en su artículo 12, el Pacto Internacional de Derechos Civiles y Políticos de 1966 artículo 17, la Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares de 1990 artículo 14 y la Convención sobre los Derechos del Niño de 1989 en

su artículo 16, esto en el plano global. En el plano interamericano se encuentra el artículo 11.2 de la Convención Americana sobre Derechos Humanos y en el europeo el artículo de la Convención Europea de Derechos Humanos (Ramírez, González y Gayo, 2017).

Actualmente existen algunos instrumentos internacionales, principalmente de índole regional, que mencionan expresamente el derecho a la protección de datos personales, algunos de estos son las Directrices de la Organización para la Cooperación y el Desarrollo Económicos sobre protección de la privacidad y flujos transfronterizos de datos de 1980 –el cual no es vinculante por tratarse de recomendaciones-, el Convenio 108 del Consejo de Europa del 28 de enero de 1981 y la Directiva 95/46/CE reemplazada por el Reglamento General de la unión europea aprobado el 17 de abril de 2016, entre otros., siendo en Europa donde se da el máximo desarrollo normativo de este derecho, llegándose a consagrar en la Carta de los Derechos Fundamentales de la Unión Europea, en su artículo 8, alcanzo su autonomía al estar en un artículo distinto al del derecho a la vida privada (Ramírez et al., 2017).

4.3. Transferencia internacional de datos

La transferencia de datos personales entre países, supone un riesgo para estos y los derechos de su titular, es por esto que a la hora de realizar transferencias de datos a terceros países, se han generado directrices por parte de algunos organismos internacionales, o se han establecido estándares de protección que garanticen la salvaguarda de este derecho.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha emitido una serie de directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales, en la cual establecen una serie de principios básicos vinculados a la protección de datos personales y restringen la transferencia con aquellos países que no ofrezcan una protección igual o superior. Pero al tratarse de recomendaciones, no es de obligatorio cumplimiento y no es jurídicamente vinculante (Valbuena Abogados, 2017).

En 1990 la Organización de las Naciones Unidas (ONU) emitió la Resolución 45/95 con algunos principios básicos de protección de datos personales de aplicabilidad mundial, en esta se establece respecto a la transferencia internacional que cuando dos o más países tengan garantías comparables de protección, la circulación debe ser tan libre como dentro de sus propios territorios (Valbuena Abogados, 2014).

Por su parte el Asia Pacific Economic Cooperation (APEC) aprobó en noviembre de 2004, su Marco de Privacidad buscando fortalecer la protección de los datos en las transferencias entre sus países miembro, se trata de un marco voluntario, reciproco y multilateral y su aplicación es de carácter flexible debido a las peculiaridades de cada país. Está inspirado en las directivas de la OCDE, aunque su estándar de protección es menor al de aquellas (Valbuena Abogados, 2017).

Así mismo, buscando proteger los datos personales, nace la Red Iberoamericana de Protección de Datos (RIPD), a raíz del encuentro iberoamericano de protección de datos celebrado en junio del 2003 en Guatemala. Sus directrices tienen como propósito que los países miembros establezcan

un marco normativo uniforme y homogéneo que permita garantizar un nivel equivalente de protección entre estos para facilitar la transferencia internacional (Valbuena Abogados, 2017).

En el plano europeo, el Reglamento General de Protección de Datos (UE) 2016/679 establece que, la legislación de los países que deseen tener transferencias internacionales de datos personales con los países miembros de la Unión Europea, debe contar con un nivel adecuado de protección. Siendo la Comisión Europea quién declara, a través de la llamada "decisión de adecuación", cuales países cuentan con el mismo (López, C., S.f.).

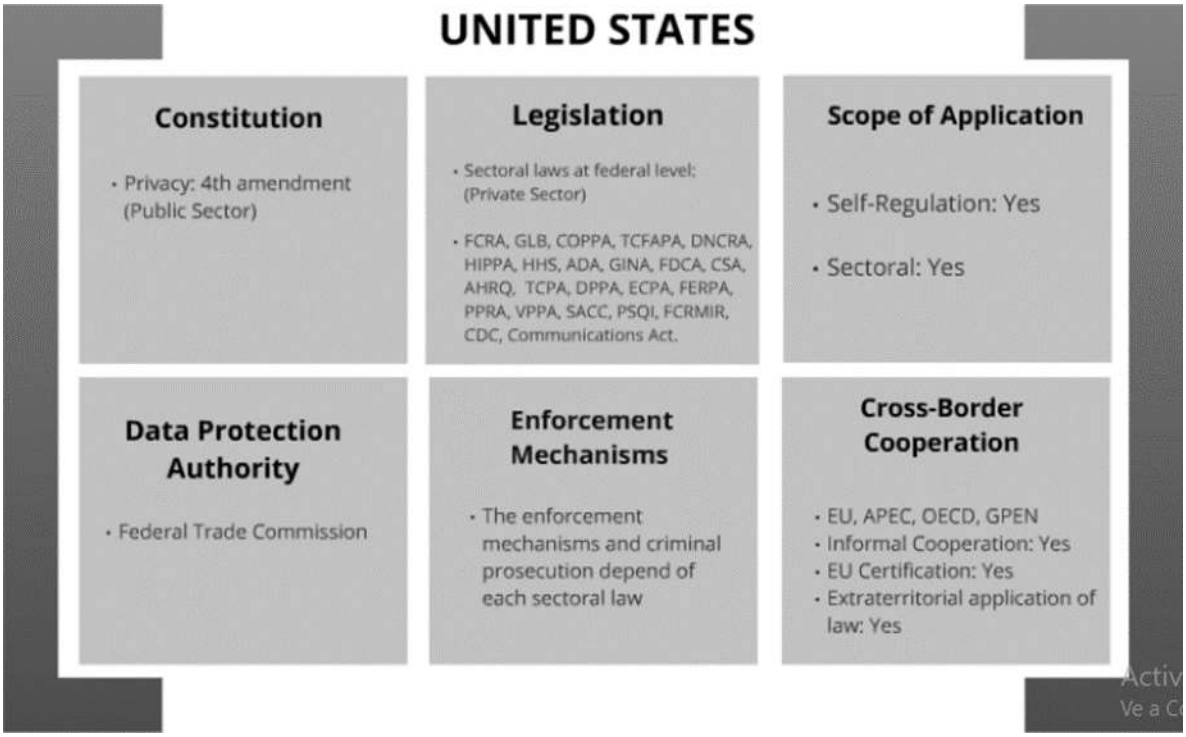
5. Protección de Datos personales en Redes Sociales e Internet

En el presente capítulo se va a realizar un análisis a las legislaciones sobre protección de datos personales existentes en el ámbito de redes sociales e internet de los países como Estados unidos, China, España, Brasil y Colombia que permitirá comprender la forma en que cada país denomina el derecho a la protección de datos personales aplicable en su territorio, mostrándose que cada uno la aborda de manera diferente y la regula igualmente de modo distinto.

5.1. Denominación de la protección de datos personales en los países EE. UU, China, España, Brasil y Colombia

Estados Unidos

Tabla 1: Protección de datos en Estados Unidos



(OEA, Organización de los Estados Americanos, 2012)

En el marco constitucional, en Estados Unidos, el derecho a la privacidad es salvaguardado por la Cuarta Enmienda de la Constitución, la cual protege la libertad e impide que se realicen injerencias arbitrarias e ilícitas en la privacidad de las personas. Regulando dicha enmienda principalmente las infracciones a la privacidad por parte del sector público y no por parte de las entidades comerciales de orden privado (OEA, Organización de los Estados Americanos, 2012). En la constitución estadounidense no se encuentra referencia expresa al derecho al Habeas Data, siendo su protección y regulación, principalmente de carácter normativo.

La legislación estadounidense no prevé el derecho al Habeas Data. Aun así, dentro de sus principios de imparcialidad en materia de privacidad de la información, se encuentra el derecho a conocer la información personal recolectada sobre la persona. Igualmente, algunas leyes como la ley sobre privacidad de la información permiten a las personas conocer los datos que sobre estos se haya recaudado, esta ley hace parte de las conocidas como "leyes de transparencia pública o de gobierno abierto" (OEA, Organización de los Estados Americanos, 2012). El mayor desarrollo legislativo en materia de privacidad de los datos, se ha dado en materia médica, en la cual se han expedido numerosas normativas.

La falta de regulación por parte del gobierno estadounidense en esta materia, se debe a que, la Comisión Federal de Comercio –Organismo encargado, entre otras funciones, de la seguridad de los datos-, ve con buenos ojos la regulación en estos temas. Considerando su viabilidad por diferentes motivos, tales como la flexibilidad y velocidad con que se adaptan las reglas al contexto social, en oposición a la relativa lentitud de las leyes, y, debido a que quienes forman parte de la industria, tienen conocimientos más especializados en la materia que quienes legislan. Siendo así que, si alguna compañía manifiesta públicamente adoptar algún tipo de autorregulación, se obliga a cumplir con esta, conforme lo establece la ley de la Comisión Federal de Comercio (OEA, Organización de los Estados Americanos, 2012).

Algunos estados de Estados Unidos han comenzado a dar pasos para la regulación del derecho al Habeas Data. El 1 de enero del año 2020, entró en vigor en California la ley de privacidad del consumidor (CCPA). Siendo esta, la primera legislación en Estados Unidos, en regular específicamente la protección de datos personales de los consumidores en línea. Dicha ley regula temas tan importantes como la recolección, el uso y la eliminación de datos personales, al igual que sanciones por la violación de los mismos (Molins Renter, 2020).

Aun así, Estados Unidos no cuenta con una ley nacional en materia de protección de datos personales, siendo la regulación de la materia, desarrollada solo por algunos de sus estados. Ante la tendencia de varios países del mundo a establecer leyes generales de carácter nacional para regular la protección de datos personales y el derecho al Habeas Data, el país norteamericano se encuentra claramente atrasado, aun y cuando en este, se crearon varias de las más grandes empresas tecnológicas que hoy operan en internet.

China

En China no se reconoce un derecho individual respecto a la intimidad, así como no se reconoce un derecho a la protección de datos personales en la Constitución de la República Popular China

de 1982, por lo que los casos que llegan a los tribunales se resuelven usando un principio del derecho civil, como lo es el derecho a la reputación (Gómez, Feijóo, y Martínez., 2017).

En noviembre del 2016, se aprobó la Ley de seguridad cibernética por parte del gobierno chino, la cual regula algunos aspectos de la protección de datos personales, entre otras disposiciones. Buscándose con esta ley la protección de la seguridad nacional, la soberanía en el ciberespacio y los derechos de sus ciudadanos (Rodrígez-Zubieta, E. P.; y Cordero-Saavedra, A. Y., 2018). Actualmente, en el año 2020, el Congreso Nacional del Pueblo (CNP) de China, se encuentra deliberando la aprobación de una regulación general de protección de la privacidad y uso de datos personales, que definiría por primera vez los límites de la privacidad y los datos personales, en un código civil en este país. El borrador de la ley define lo privado como todo aquello que el individuo no está dispuesto a dar a conocer a otras personas, no pudiendo y a lo que no pueden acceder terceros sin su consentimiento (Pérez, M., 2020).

España

En España los datos personales de las personas en internet son protegida mediante el derecho a la protección de datos personales en bases de datos automatizadas. Solo fue hasta el año 2000, que el Tribunal Constitucional Español, mediante la Sentencia 292/2000, reconoció el derecho a la protección de datos como un derecho autónomo. Antes de esto, la jurisprudencia constitucional, se basó en el leading case de la STC 254/1993, para partir del derecho a la intimidad y añadirle una vertiente informática. Aun así, el derecho a la intimidad se quedaba corto para proteger los datos personales, ya que este solo pretende preservar una esfera de la libertad del individuo de los poderes del Estado, por lo que la mera abstención de actuar de este, garantizaba el derecho. Por su parte, el derecho a la protección de datos, no solo protege frente a la actuación de los poderes públicos, sino también frente a la actuación de otros particulares; además de garantizar facultades de actuación para la protección del derecho (Roig, 2009).

A nivel legislativo, el derecho a la protección de los datos personales tuvo sus orígenes en la Ley Orgánica 5 del 29 de octubre de 1992, conocida como LORTAD, y la cual regulaba el tratamiento automatizado de datos personales. Posteriormente fue reemplazada por la Ley Orgánica 15 del 5 de diciembre de 1999, la cual regulaba la protección de datos personales, siendo expedida esta para acoplar la legislación española a la Directiva 95/46/CE del 24 de octubre de 1995, emitida por el Parlamento Europeo y del Consejo, la cual tenía por objeto procurar que la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos dentro de la Unión Europea, asegurándose que en los casos de transferencia internacional, el país destinatario de los datos tuviera salvaguardas para su protección, las cuales se adecuaran a dicha Directiva (Ley Orgánica Española 3, 2018). Esta ley a su vez fue reemplazada por la Ley Orgánica 3 del 5 de diciembre de 2018, sobre protección de datos personales y garantía de los derechos digitales, esta norma tiene por objeto adaptar la legislación española al Reglamento (ue) 679 del 27 de abril de 2016 del Parlamente europeo y del Consejo, conocido como Reglamento General de Protección de Datos (RGPD), con el cual se pretende superar los obstáculos que impidieron materializar los fines de la Directiva 95/46/CE, haciendo las disposiciones de dicho reglamento, de aplicación directa, lo cual no ha impedido a cada Estado aprobar sus propias normas, adaptando y complementando la nueva regulación, como es el caso de España con la Ley Orgánica 3 de 2018 (Rodríguez, Junio, 2019).

Por su parte, en el campo constitucional, la Constitución Española (CE) en su artículo 18 numeral 4, establece la limitación del uso de la informática para garantizar el honor y la intimidad ciudadanos, al igual que el pleno ejercicio de sus derechos. Precepto que completa el artículo 18, junto con sus otros tres numerales, como lo son el numeral 1, que protege el derecho al honor, a la intimidad y a la imagen; el numeral 2, que protege la inviolabilidad del domicilio; y el numeral 3, el cual protege el secreto de las comunicaciones. El artículo 18 de la Constitución Española, con sus respectivos numerales, hace parte del capítulo de los derechos fundamentales de la ciudadanía, lo cual es reflejo de su importancia (Constitución española, 1978).

Brasil

En Brasil, el derecho a la protección de datos personales, tiene su origen en la Constitución Política de la República Federativa del Brasil de 1988, que en su artículo 5. LXXII, consagra que se concederá Habeas Data en aquellos casos que sirva para asegurar el conocimiento de informaciones sobre la persona que consten en bases de datos de entidades gubernamentales o de carácter público, o para la rectificación de datos, cuando no se prefiera hacer mediante otro procedimiento. De igual manera, el mismo artículo constitucional, en su literal X, consagra la inviolabilidad de la intimidad, la vida privada, el honor y la imagen de las personas, estableciendo una indemnización en caso de daños materiales o morales por su violación (Constitución Política de la República Federativa del Brasil, 1988).

En el ámbito legislativo, tras largos debates e intentos de aplazamiento de la entrada en vigencia de su ley nacional de protección de datos, finalmente el 18 de septiembre del año 2020, entró en vigor la Ley General de Protección de Datos brasileña, siendo la primera ley general en la materia del país. Pero su vigencia no es total, pues la aplicación de las sanciones por su incumplimiento se pospuso hasta agosto del 2021 (Carreño, 2020), fecha a partir de la cual se espera que entre completamente en vigencia esta nueva ley.

Colombia

En Colombia, antes de la constitución política de 1991, no había una consagración expresa del derecho intimidad, el cual solo fue consagrado en la carta magna y elevado al grado de derecho constitucional, a partir de la constituyente del 91. La Constitución Política Colombiana consagra el derecho a la intimidad en su artículo 15, al consagrar: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar…” (Constitución Política Colombiana, 1991, art. 15).Pudiendo desprenderse de este mismo artículo, en otro sus apartes, el derecho a la protección de datos personales, o como es conocido a en Colombia, Derecho al Habeas Data, el cual es consagrado por la Constitución Política así: “derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas” (Constitución Política Colombiana, 1991, art.15). Siendo este derecho en sus comienzos, ligado al derecho a la intimidad.

Anteriormente el Derecho al Habeas Data era considerado una garantía al derecho a la intimidad que va muy de la mano con la vida privada y familiar de una persona, sin embargo, la Corte Constitucional ha manifestado que el Derecho al Habeas Data es un derecho personalísimo que permite crear un equilibrio entre el titular del dato sometido a tratamiento y aquel encargado y responsable de los bancos de datos donde son depositados todos los datos personales (Gordillo y Restrepo, 2004).

El derecho al Habeas Data, no nace como derecho autónomo, sino a partir de 1995. Antes de este año la jurisprudencia constitucional había tenido dos líneas distintas de interpretación del derecho al habeas data. Bajo la primera línea, este derecho fue interpretado como una garantía del derecho a la intimidad. Bajo la segunda línea, se interpretó como una manifestación del derecho al libre desarrollo de la personalidad. Posteriormente, con la Sentencia SU-082 de 1995, nace la tercera línea interpretativa, la cual concibe el derecho al habeas data como un derecho autónomo, el cual tiene como núcleo central la autodeterminación informática y la libertad. Según lo afirma la Sentencia C-748 de 2011, esta tercera línea es la que ha prevalecido desde entonces. (CCC, Corte Constitucional Colombiana, Sent C-748, 2011).

El derecho al habeas data, entendido como derecho autónomo, es aquel derecho que:

> "permite a las personas naturales y jurídicas conocer, actualizar y rectificarla información que sobre ellas se haya recogido en bancos de datos y en archivos de entidades públicas y privadas. De la misma manera, este derecho señala la obligación de respetar la libertad y demás garantías constitucionales en el ejercicio de las actividades de recolección, tratamiento y circulación de datos" (CCC, Corte Constitucional Colombiana, Sent T-176 A, 2014)**.**

Además, la Corte Constitucional Colombiana ha señalado que, aunado a la anterior definición, este derecho comprende al menos las siguientes prerrogativas:

> "a) El derecho a conocer las informaciones que a ella se refieren; || b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; || c) El derecho a rectificar las informaciones que no correspondan a la verdad.", e incluye el derecho a la caducidad del dato negativo" (CCC, Corte Constitucional Colombiana, Sent SU-O82, 1995).

El derecho a la intimidad, a su vez, es un derecho que empezó ser tenido en cuenta y a verse la necesidad de su protección, a partir la revolución francesa y la norteamericana. En el plano colombiano, solo se consagró este derecho de manera expresa, con la Constitución de 1991, la cual en su artículo 15 plasma: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar" (Constitución Política Colombiana, 1991, art.15).

Al referirse a este derecho, La Corte Constitucional colombiana ha dicho que se trata de un derecho absoluto, que no puede ser desconocido por ni por los particulares, ni por el estado, y el cual "… alude al derecho obvio de todo individuo a rehusar que cualquiera, Estado o particulares, tengan

acceso a la esfera interna de la persona". (CCC, Corte Constitucional Colombiana, Sent T-176, 1995).

Este derecho y el derecho al habeas data son independientes el uno del otro, pero, aun así, la recolección de cierta información puede afectarlos a ambos, como es la información relacionada con la vida privada de la persona. La Corte Constitucional Colombiana (2016) ha precisado aquellos aspectos que tocan con la vida íntima de la persona así:

> "[…] constituyen aspectos de la órbita privada, los asuntos circunscritos a las relaciones familiares de la persona, sus costumbres y prácticas sexuales, su salud, su domicilio, sus comunicaciones personales, los espacios limitados y legales para la utilización de datos a nivel informático, las creencias religiosas, los secretos profesionales y en general todo "comportamiento del sujeto que no es conocido por los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación" que éstos tienen de aquel"(CCC, Corte Constitucional Colombiana, Sent T-050, 2016).

A nivel normativo, desde su consagración en la Constitución Política, se trató de regular el derecho al Habeas Data mediante múltiples iniciativas legislativas, las cuales, por una u otra razón, no llegaron a convertirse en ley, dejando por un largo tiempo sin una regulación concreta este derecho. Algunas de estas iniciativas legislativas que se presentaron en Colombia desde su consagración en la Constitución hasta proferirse finalmente una regulación normativa en la materia, son:

Tabla 2 Protección de datos en Colombia

PROYECTO	OBJETO	CONCLUSION
1. Proyecto de Ley senado 12 de 1993 y Cámara 127 de 1993.		El cual fue declarado inexequible por la Corte Constitucional en la revisión previa a la Sanción Presidencial. prevista en el artículo 152, por sentencia C-008/95.
Proyecto de Ley Estatutaria número 201 de 2003 Cámara, 071 de 2002 Senado	"Por la cual se regula el derecho de acceso a la información de interés público, en particular la de carácter comercial, financiero, la que tiene que ver con el cumplimiento de obligaciones fiscales y parafiscales y con el pago de servicios públicos domiciliarios, y se dictan otras disposiciones"	No se convirtió en Ley de la República por falta de trámite.
Proyecto de Ley Estatutaria número 074 de 2003 Cámara, 064 de 2003 Senado.	"Por la cual se regula integralmente el derecho fundamental al hábeas data y demás libertades y derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales a través de bases de datos públicas y privadas, y se dictan otras disposiciones"	No se convirtió en Ley de la República por falta de trámite
Proyecto de Ley Estatutaria número 143 de 2003 Senado.	"Por la cual se dictan disposiciones para la protección de datos personales y se regula la actividad de recolección, tratamiento y circulación de los mismos"	Tampoco se convirtió en Ley por cuanto fue archivado en sesión plenaria del Senado el 9 de junio de 2004.
Proyecto de Ley Estatutaria número 139 de 2004 Cámara.	"Por la cual se regula integralmente el derecho fundamental al hábeas data y demás libertades y derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales a través de bases de datos públicas y privadas, y se dictan otras disposiciones"	No tuvo debate en la Comisión Primera de la Cámara al ser retirado por su autor en sesión del 31 de mayo del año 2004.

(Iguarán Osorio, M.Á.; y Muñoz Jiménez, R., 2012)

Estos fueron algunos de los proyectos legislativos que intentaron dar una regulación normativa al Habeas Data, pero que no llegaron a convertirse en ley. Siendo el final de estos intentos legislativos, el proyecto de Ley Estatutaria No. 221/2007 del Senado, el cual fue aprobado por el congreso y termino por convertirse en la Ley 1266 del 31 de diciembre de 2008, conocida como Ley de Habeas Data, por la cual se dictan disposiciones generales sobre el Habeas Data y se regula el manejo de la información contenida en bases de datos personales (Iguarán Osorio, M.Á.; y Muñoz Jiménez, R., 2012). Siendo esta la primera Ley de Habeas Data en el país, pero la cual contaba con ciertas limitaciones, debido a que fue expedida principalmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países. En el año 2012, por medio de la Ley 1581 del 18 de octubre de 2012, se dictaron las disposiciones generales para la protección de datos personales, aplicable a todos los ámbitos de la recolección de datos personales (Colombian Legal Corporation, 2019). Ley que fue a su vez, reglamentada parcialmente, por el Decreto No. 1377 del 27 de junio de 2013.

Capítulo II. Indicadores sobre protección de datos personales en redes sociales e internet (EEUU, China, España, Brasil y Colombia)

Indicador # 1. Existencia de una ley unificadora de la legislación sobre datos personales

Estados Unidos

Estados Unidos no cuenta con una legislación nacional sobre protección de datos personales, dejando este tema principalmente en manos de la autorregulación del mercado, y de las leyes que al respecto expida para sí cada estado. La ley más completa en la actualidad en el país norteamericano, es el California Consumer Privacy Act (CCPA) o Ley de Privacidad del Consumidor de California, aprobado en el 2018, y la cual entró en vigencia a partir de enero del 2020. Siendo por esto, dicha ley, el marco de referencia principal para el análisis de este y los demás indicadores del presente capítulo.

China

En China la legislación nacional en materia de protección de datos personales se encuentra regulada mediante la Ley de Ciberseguridad China, la cual entro en vigencia el 1 de junio del año 2017 y contiene las disposiciones relativas a la seguridad de los datos en internet.

España

En España se encuentra unificación en la materia de protección de datos personales, gracias a la Ley Orgánica de Protección de Datos (LOPDGDD) expedida por este país para acoplarse a las disposiciones del Reglamento Europeo. Dicha ley fue aprobada en el senado español el 5 de diciembre de 2018, fue publicada en el boletín oficial del estado (BOE) el 6 de diciembre y entro en vigencia el 7 de diciembre del mismo año (Sánchez, 2018).

Brasil

Brasil cuenta con unidad legislativa en la materia, regulando lo relativo a la protección de datos personales, mediante la Ley General de Protección de Datos Personales (LGPD). Ley que entró en vigencia el 18 de septiembre de 2018.

Colombia
En Colombia, la protección de datos personales se encuentra regulada a través de Ley Estatutaria 1581 del 18 de octubre 2012, la cual fue reglamentada a su vez por el Decreto 1377 del 2013, decreto que amplía ciertos aspectos de la protección de datos personales y por medio del cual se derogan las disposiciones que le sean contrarias.

Indicador # 2. Obligación de indicar con qué fin se recoge la información para el tratamiento

Estados Unidos

El estado de California, en Estados Unidos, en la sección 999.305 de la ley de privacidad del consumidor, establece la obligación, cuando se van a recolectar los datos, de generar un aviso que debe contener las categorías de datos que se recolectarán y los fines con que será usada dicha información, lo cual deberá constar en un lenguaje sencillo y entendible (Ley de privacidad del consumidor de California, 2020).

China

En lo que respecta a la obligación de indicar con qué fin se recoge la información para el tratamiento, el artículo 41 de la ley de Ciberseguridad china, establece la obligación para los operadores de la red, al recopilar la información, de expresar tanto el propósito como el método, alcance y uso que se le dará, y ser estos explícitos e informados al titular de los datos, ligando la recolección de los datos a los principios de legalidad, legitimidad y necesidad y a la obtención del consentimiento del titular (Ley de Ciberseguridad China, 2017).

España

En La legislación española, esta obligación se encuentra consagrada en el artículo 6 de la ley orgánica de protección de datos, en el cual se establece en el numeral 1 que el consentimiento para el tratamiento debe ser libre, especifico, informado e inequívoco, en el numeral 2 que cuando el consentimiento para el tratamiento se otorgue para una pluralidad de fines debe constar de manera específica e inequívoca que es para todos ellos. Así mismo, el artículo 11 de la misma ley establece que, acorde con el artículo 13 del reglamento general de protección de datos europeo, al momento de recolectar los datos se le debe informar a su titular, entre otras cosas, la finalidad del tratamiento (Ley Orgánica de Protección de Datos de España, 2018).

Brasil

En Brasil, el artículo 6 de la ley general de protección de datos consagra algunos principios para el procesamiento de datos personales, entre los cuales se encuentra el principio de propósito, según

el cual, el tratamiento debe ser llevado a cabo con los fines informados al titular. El artículo 7, numeral 1, establece que solo se puede llevar a cabo el tratamiento si se ha otorgado consentimiento por parte del titular, y, en este mismo sentido, el artículo 8, de la ley en mención, establece que el consentimiento para tratar los datos debe referirse a fines específicos, sin permitirse las autorizaciones genéricas para el tratamiento, las cuales en caso de presentarse serán nulas. Sin embargo, no se establece la obligación de indicar que datos serán recolectados (Ley General de Protección de Datos Personales de Brasil, 2020).

Colombia

La ley 1581 de 2012, entre sus principios para el tratamiento de datos personales establecidos en el artículo 4, consagra en el literal b su principio de finalidad según el cual, el tratamiento debe obedecer a una finalidad legitima, acorde con la constitución y la ley, la cual debe ser informada al titular de los datos. Así mismo, el artículo 9 de la ley en mención, estipula que en el tratamiento de los datos se requiere la autorización previa e informada del titular de los mismos, y el artículo 12, el deber de informar al titular por parte del responsable del tratamiento, al momento de solicitar su autorización, el tratamiento al cual serán sometidos los datos y la finalidad de este *(Ley 1581, 2012).*

El Decreto 1377 del 2013 de Colombia, regula esta obligación en su artículo 5, estableciendo que el responsable del tratamiento deberá a más tardar en el momento de la recolección de los datos, informar que datos serán recolectados, al igual que las finalidades para las que serán tratados y deberá solicitar la autorización de su titular para la recolección y tratamiento de los mismos (Decreto 1377, 2013).

Indicador # 3. Limitación del uso y tratamiento de los datos personales recolectados

Estados Unidos

En el California Consumer Privacy Act, no se encuentra ninguna disposición que de manera expresa limite el tratamiento de los datos personales recolectados solo para aquellos fines que se informaron en la recolección, así como tampoco, ninguna que limite la recolección de datos, solo a aquellos necesarios para la prestación del servicio (Ley de privacidad del consumidor de California, 2020).

China

En lo que respecta a la limitación del uso y tratamiento de los datos personales recolectados, la República Popular China, en su ley sobre ciberseguridad, estipula en su artículo 41 que no se podrá recolectar información personal que no se relacione con los servicios que se prestan, así como también indica que la utilización de la información recaudada estará supeditada al acuerdo con los titulares de la misma, la cual según se dice en este mismo artículo, al momento de su recolección debió limitarse a aquella necesaria para la prestación del servicio, estando ligada la utilización de

los datos recolectados a los principios de legalidad, legitimidad y necesidad (Ley de Ciberseguridad China, 2017).

España

Del artículo 6 de la ley orgánica de protección de datos española, se desprende que el tratamiento de los datos personales debe estar basado en el consentimiento previo del titular de los mismos, el cual deberá ser libre, especifico, informado e inequívoco. Así mismo, se establece que, la ejecución del contrato para la prestación del servicio, no podrá estar supeditado a que se consienta el tratamiento de datos personales del individuo, para aquellas finalidades que no sean propias y necesarias del contrato. Lo que obligaría a que los datos recolectados y tratados sean solo los necesarios para desarrollar el objeto del contrato (Ley Orgánica de Protección de Datos de España, 2018).

Brasil

Por su parte, Brasil, en su ley de datos personales, toca este tema en el artículo 6, numeral 1, en el cual prohíbe que se le dé un tratamiento a la información distinto de aquel para el cual fue recolectada; en su numeral 2 establece que el tratamiento debe ser compatible con los fines que le fueron informados al titular de esta, y, en el numeral 3, establece que el tratamiento de los datos debe ser el mínimo necesario para garantizar que se cumpla con los fines estipulados, prohibiendo cualquier tratamiento excesivo respecto a los fines perseguidos.

Por otra parte, el artículo 10 de la citada ley establece que solo fines legítimos pueden justificar el tratamiento de datos personales y solo pueden ser procesados aquellos datos estrictamente necesarios para el fin previsto (Ley General de Protección de Datos Personales de Brasil, 2020).

Colombia

En Colombia, la limitación del uso y tratamiento de los datos personales recolectados, se establece en el artículo 4 del Decreto 1377 del 2013, el cual establece que, la recolección de datos debe limitarse solo a aquellos datos que sean pertinentes y adecuados para cumplir con las finalidades para las cuales son recolectados. Por su parte, el artículo 11 del mismo decreto, establece que los responsables del tratamiento de la información, solo podrá, recolectar, almacenar y usar los datos personales, de acuerdo con las finalidades que justificaron el tratamiento (Decreto 1377, 2013).

En este mismo sentido, la ley 1581 del 2012 en su artículo 4, en el cual consagra los principios rectores del tratamiento de datos personales, en su literal b sobre el principio de finalidad, establece que el tratamiento debe obedecer a una finalidad legítima y debe ser informada al titular (Ley 1581, 2012).

Indicador # 4. Posibilidad de eliminación de los datos

Estados Unidos

En el caso de Estados Unidos, la eliminación de datos personales está contenida en la Ley California Consumer Privacy Act (CCPA) desarrollada ampliamente desde su artículo 1º Lit.(q) y art 2º en su sección § 999.308, donde define tal disposición, y lo despliega procedimentalmente en su artículo 3º sección § 999.312. En Estados Unidos cada empresa tiene la obligación legal de contar con un mecanismo de solicitudes por medio de correo electrónico, o llamada gratuita directamente a la empresa, para que los titulares de los datos personales tengan facilidad para solicitar la eliminación de sus datos personales objeto de tratamiento y comercialización. En los casos que no sea posible identificar al titular del dato a eliminar, la empresa puede conservar tales datos, o en caso de que el solicitante no lleve a cabo en debida forma el procedimiento establecido en la empresa para la eliminación de sus datos, la misma podrá conservarlos también, pero, antes de seguir vendiendo sus datos debe primero consultar con el titular si desea optar por la comercialización o no.
A parte de la solicitud de eliminación, los titulares deben hacer un segundo escrito reiterando la necesidad y voluntad de que sus datos sean eliminados y las empresas deberán actuar de conformidad, notificando la recepción de tales solicitudes y dando respuesta máxima dentro de los 90 días siguiente

En el país en mención, tienen en cuenta la información recopilada de los hogares, como lo son los datos personales de un grupo familiar, donde los menores de edad están bajo consentimiento de los padres de familia. Se llevará a cabo el mismo procedimiento que con la solicitud, pero la misma debe realizarse en conjunto con todos los miembros de tal hogar. Los encargados de la eliminación de los datos personales deben primero cerciorarse de que las personas que hacen solicitud de eliminación sean las mismas de que la empresa ha recopilado los datos, para esto, la empresa puede acceder a datos sensibles con el fin de tener certeza de la identificación de tal titular, de lo contrario toda solicitud será rechazada (Ley de privacidad del consumidor de California, 2020).

China

Por parte de la República Popular China, la eliminación de datos personales es desarrollada en los artículos 43, 50 de la Ley de Ciberseguridad.
En este ámbito se tiene permitido que, si cualquier persona encuentra prácticas ilícitas con respecto de sus datos personales por parte del operador, está en todo el derecho de solicitar su eliminación. Los operadores de la web tienen el deber de tomar nuevas medidas técnicas para el tratamiento que permita garantizar mejor la seguridad de los datos. En ningún caso el operador para la recolección de los datos establecerá ningún sistema malicioso que deje recopilar información prohibida por la ley y menos su publicación, esto es razón de eliminación inmediata de tales datos e incluso se debe de dejar de prestar el servicio por parte del operador infractor *(Ley de Ciberseguridad China, 2017)*.

España

En España, la posibilidad de la eliminación de los datos personales se encuentra regulada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea, en su artículo 17 desarrolla ese derecho a la supresión o como también es denominado en Europa, el derecho al olvido.

El titular de los datos personales sometidos a tratamiento podrá en cualquier momento solicitar la eliminación debido a que los datos ya no resultan necesarios para el tratamiento para el que fue recopilados, también en razón de que el titular ya no de consentimiento para el tratamiento de los mismos, que el titular encuentre actuaciones ilícitas respecto del uso de sus datos personales, entre otras razones, como por motivo de obtener provecho económico ilícito por el tratamiento por parte del operador (Ley Orgánica de Protección de Datos de España, 2018).

Brasil

En Brasil, la posibilidad de eliminar los datos por decisión del titular no se encuentra desarrollado ampliamente, sin embargo, se regula someramente en tres artículos de la ley de protección de datos de Brasil, como son el artículo 16, artículo 18º sección IV, VI y artículo 52 sección VI, éste último como sanción.

La eliminación de los datos será llevada a cabo cuando los datos personales ya hayan sido objeto de tratamiento y se haya culminado su manipulación, puede ser solicitado por parte del titular del dato la eliminación de los mismos, siempre y cuando no haya autorización de conservarlo debido a que el dato se ha anonimizado, de lo contrario no será posible su conservación. La conservación solo será posible cuando sea por mandato legal, por motivos de investigación sin perjuicio de divulgación de datos personales de los titulares que permitan su individualización, entre otros aspectos en los cuales es lícita tal actuación. A solicitud de parte, el titular puede exigir en cualquier momento que los datos que ya fueron objeto de estudio sean eliminados, al igual que aquellos impertinentes, innecesarios, excesivos, inexactos u obsoletos (Ley General de Protección de Datos Personales de Brasil, 2020).

Colombia

En Colombia la eliminación de los datos por requerimiento del titular de estos se ve reflejado concretamente desde el artículo 8º Lit. e, art 15 y art 18 Lit. c de la ley habeas data (Ley 1581/2012) y el Decreto 1377/2013 en los artículos 9 y 10. La Superintendencia tiene el deber de adelantar investigaciones sobre las vulneraciones e infracciones a la ley e inmediatamente por petición de parte o de oficio, puede ordenar toda medida que garantice el efectivo ejercicio del derecho al habeas data, la supresión de los datos es una de ellas. Será obligatorio la supresión de los datos en los casos donde se desconocen los principios, derechos constitucionales y garantías legales que persigue las mencionadas leyes, también será obligatorio la eliminación a libre disposición de las partes, por medio de reclamo ante el órgano competente solicitando la eliminación de sus datos personales.

Si después de entrar en vigor el Decreto 1377/2013, los encargados del tratamiento de datos personales no informan a los titulares de los mismos respecto de revocar el consentimiento para seguir con el uso, estarán obligados a eliminar todos los datos personales que tengan en su radar por omitir tal transparencia con el titular. De igual manera, éste último puede solicitar la eliminación de sus datos en cualquier momento si así lo considera a menos de que esté bajo un deber legal de permanecer sin eliminar. Este Decreto protege al titular respecto de la libertad de

eliminar sus datos y regula sus efectos en el procedimiento que se desarrolla en la Ley 1581/2012 (Decreto 1377, 2013).

Indicador # 5. Transferencia Internacional y Transferencia a terceros

Estados Unidos

Estados Unidos permite la trasferencia de la información a terceros. Está contenida en la Ley California Consumer Privacy Act (CCPA) en la sección 999.308 Lit. (C)(g), que es denominada Divulgación o venta de información personal.

En Estados Unidos se considera la transferencia de información a terceros como una comercialización de esta, es decir, que los datos personales son vendidos a terceros con el fin de dar un tratamiento a los mismos y sacar cierta información que le concierne a las mismas empresas que los compran. Para su comercialización, cada empresa debe de tener almacenado e identificado cada categoría de información personal que ha divulgado con fines comerciales, como también debe de contar con la identificación de las categorías de los terceros a los cuales se vendió la información (Ley de privacidad del consumidor de California, 2020).

La empresa que se dedique a la comercialización de los datos personales debe de notificar siempre que se dedica a tal fin y ofrecer la opción de optar por no participar en la venta de la información por parte de los titulares según lo establecido en la sección 999.306 de la misma ley o siendo los datos ya vendidos o tratados por terceros, pueden por medio de una solicitud de exclusión voluntaria, exigir que los datos personales no sea vendido a terceros según lo establecido en la sección 1798.120 del Código Civil de California (Código Civil de California, 1872).

China

En China, la transferencia internacional de datos no está permitida libremente, pues en su artículo 37 de la Ley de Ciberseguridad se manifiesta que la información personal recopilada se almacenará en el territorio nacional, no podrá ser compartida con ningún otro país si no se es realmente necesario. En su artículo 66 sanciona a aquellos operadores que compartan información recopilada en el país con países terceros, enviándolos a corregir y estableciendo una multa que puede ir desde hasta 100.000 yuanes hasta ordenar cerrar sitios web y suspender negocios relacionados (Ley de Ciberseguridad China, 2017).

España

Por su parte, España considera para la transferencia internacional de los datos, que el país destino tenga una regulación adecuada para su protección. La transferencia internacional se encuentra consagrada en Ley Orgánica 3/2018 en su Disposición Adicional Quinta, en su Título VI, Art 40 en adelante, que a su vez es regulada también por el Reglamento (UE) 2016/679, como ya se dijo ocasiones pasadas, este Reglamento Europeo complementa la mencionada ley nacional de protección de datos personales, estableciéndose que cualquier país que quiera tener transferencia

de datos con España debe contar con un nivel adecuado de protección, según los estándares de la Unión Europea (Ley Orgánica de Protección de Datos de España, 2018).

Brasil

En Brasil, la transferencia internacional de los datos está permitido y es regulado por el artículo 33 de la ley de protección de datos. La transferencia internacional de los datos está permitida en la medida de que el tercer país que recibe la información contenga una adecuada protección de los datos personales para poder llevarse a cabo tal transferencia, debiendo dar garantías de cumplimiento de los principios y ser compatible con el régimen de protección de datos de Brasil y que aparte cuente con lo establecido en el artículo 33 apartado II:

a) cláusulas contractuales específicas para una transferencia dada;
b) cláusulas contractuales estándar;
c) estándares corporativos globales;
d) sellos, certificados y códigos de conducta emitidos regularmente

El Gobierno Brasileño, deberá evaluar todas las normativas legales y principios sobre protección de datos del país destino. Lo que resulta necesario para la transferencia internacional de datos personales para garantizar una debida protección.

La transferencia internacional será permitida también cuando sea netamente necesario, como lo es, para llevar a cabo el ejercicio del derecho internacional, cuando de la transferencia dependa la vida o seguridad del titular, por autorización de órgano de control, por cooperación internacional entre otras razones lícitas que permiten el ejercicio de esta actividad (Ley General de Protección de Datos Personales de Brasil, 2020).

Colombia

En Colombia, Está prohibido por la legislación colombiana la transferencia de datos a terceros países que no dispongan con un nivel de protección de datos personales igual o superior al de Colombia. Tales prohibiciones no serán aplicables cuando el mismo titular haya dado su consentimiento de transferencia, por razones de salud del titular, por razones establecidas en tratados internacionales en los que Colombia es parte, por el interés público, entre otras razones por las cuales es posible la transferencia en Colombia.

En lo establecido al respecto en el Decreto 1377/2013, para la transferencia de los datos personales a terceros países, es obligatorio contar con un contrato de transmisión donde se vea lo plasmado en el artículo 26 de la Ley Habeas Data, que es asegurarse de que el país al que se van a transferir los datos tenga un nivel de protección igual o mayor al de Colombia (Decreto 1377, 2013).

Indicador # 6. Protección de niños, niñas y adolescentes en internet

Estados Unidos

Por otra parte, en Estados Unidos a partir del 2013 fue que se empezó a proteger a los niños, niñas y adolescentes en la esfera de las redes sociales e internet, con la ampliación de la Ley COPPA (Children's Online Privacy Protection Act). La Comisión Federal de Comercio es el ente encargado de vigilar las páginas web dirigidas a menores de edad, validando su contenido, características, publicidad y demás para reportar posibles casos de vulneración de derechos del menor de edad.

En Estados Unidos es notable la exigencia que se maneja con la protección de los datos de los menores, pues en la sección §312.5 de la Ley COPPA se encuentra contenido todo lo relacionado con el consentimiento de los padres; hemos mencionado en varias ocasiones que el consentimiento es un elemento integral del tratamiento, uso y manipulación de los datos personales y es de suma importancia que siempre se cuente con él, porque contar con éste es dar a entender que el titular de los datos o en éste caso los padres del menor, están debidamente informados y notificados del tratamiento y han otorgado su permiso para tal actividad. En la Ley de protección datos del menor en Estados Unidos se exige al operador de internet que previo a obtener el consentimiento de los padres realice un aviso que deberá contener toda la información pertinente y detallada relacionada del tipo de información que se pretende tratar y con qué fin. Para la obtención del consentimiento es obligatorio que el mismo sea verificado, es decir, que se tenga la certeza de que la persona que firmó el consentimiento para el tratamiento de los datos del menor sí sea el padre o la madre y no otra persona; para ello se puede llevar a cabo un sistema de ''puerto seguro'' como es denominado en la sección §312.11, que es que un método de obtención del consentimiento que debe cumplir con una protección igual o mayor de la ley en mención, dicho sistema de puerto seguro puede contener varios requisitos, como lo es un tener un formulario para ser firmado, que haya la posibilidad de llamar o realizar videoconferencia con el fin de tal verificación, entre otros. Es entonces como en este país protegen a los menores frente al uso de internet.

Tal y como en los análisis anteriores, no se puede recolectar, ni manipular datos sin el consentimiento de sus padres o representantes legales. Por lo anterior en YouTube, por ejemplo, cualquier creador de contenidos para niños tiene que cumplir con varios requisitos, como especificar cuáles son contenido para niños, con el fin de que se eliminen comerciales publicitarios, se elimine la posibilidad de dar «me gusta» y de tener ingreso a chats directos con otras personas (Children´s Online Privacy Protection Act, 2013).

China

En el caso de la República Popular China, existe la Ley de Ciberseguridad en la que se dedica únicamente un solo artículo a los niños, niñas y adolescentes, el cual es el art 13 y en su Ley denominada Reglamento sobre la protección de la información personal de los niños en línea, en donde enfocan su interés en el crecimiento integral de los menores, sancionando las practicas desfavorables que les proporcionen un grave riesgo. También procura garantizar un ambiente sano para la participación de los niños, niñas y adolescentes en el internet, sin embargo, en el 2019 se crea un nuevo reglamento sobre la protección de la información personal de los niños niñas y adolescentes en internet, convirtiéndose en la primera ley que regula a profundidad y de manera integral este ámbito en el país. El consentimiento sigue siendo un elemento esencial para la protección y el tratamiento de los datos, para los menores no será posible la navegación libre en

internet y redes sociales si no hay un tutor o representante que lo supervise. En el desarrollo de esta nueva ley, se encuentra un marco regulatorio propio con reglas para la recolección, uso, transferencia y tratamiento de los datos personal de los menores de edad, estas reglas están ajustadas a este público, aumentando el nivel de protección y seguridad para el niño, niña o adolescente. (Reglamento sobre la protección de la información personal de los niños en línea, 2019).

España

En España la protección de datos de los menores de edad en internet está regulada en la Ley Orgánica 3/2018 en su artículo 84, en conjunto con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo desde su artículo 8º.
Se observa que el consentimiento sigue siendo una pieza importante en la protección de datos, y en los niños, niñas y adolescentes debe de ser aún más evidente, pues los menores suponen una especial vigilancia para el Estado y sus familiares. Por eso el consentimiento no está a suerte solo del menor; pues en ciertos casos es necesaria la participación de los representantes legales o padres para confirmar tal consentimiento, a menos que tenga 16 años o más, pues según el Reglamento 2016/679 (UE) su consentimiento sería lícito en tal caso.
Observamos que el consentimiento sigue siendo una pieza importante en la protección de datos.

Respecto de la protección en redes sociales e internet de los niños, niñas y adolescentes se encuentra desarrollado en la ley de protección de datos española, en su artículo 84, donde estos están bajo supervisión estricta de sus padres o representantes legales, ya que es esencial entre otras cosas, para afianzar su dignidad y derechos fundamentales. Por otra parte, también es responsabilidad de cualquier persona natural o jurídica que se desempeñen profesionalmente con menores de edad en cualquier ámbito que implique la utilización de medios de la sociedad de la información, la protección de estos.

Brasil

En Brasil por su parte, la protección de datos de los niños, niñas y adolescentes tiene lugar en la Ley 13.709/2018, en su sección III, artículo 14.

En Brasil el consentimiento está solo en cabeza de los padres, si no es otorgado no es posible llevar a cabo tratamiento alguno, a menos que sea por seguridad del menor o que sea sumamente necesario para los intereses de estos, sin posibilidad de almacenar ninguno de los datos usados.

En relación con las redes sociales, aplicaciones de internet y juegos, para que un menor pueda crear su usuario, no se le solicitarán datos más que los que son básicos y necesarios para tal fin y no será obligatorio la participación de los padres para elaborar una cuenta, pues basta con los datos mínimos que no afectan la seguridad del niño, niña o adolescente, sin embargo, el operador de las paginas para menores, tiene la obligación de verificar que el consentimiento sea manifiesto por el responsable del menor (Ley General de Protección de Datos Personales de Brasil, 2020).

Colombia

Por su parte, Colombia, en la protección de datos personales de los menores cuenta con la Ley 1581 de 1012 en su art. 7º y el Decreto 1377 de 2013 en su artículo 12º. Se prohíbe en ambas disposiciones todo uso de datos personales de menores de edad para garantizar su seguridad, sin contar aquellos datos que por su naturaleza son públicos como el estado civil y ocupación. (Decreto 1377, 2013).

El Gobierno Nacional Colombiano y organizaciones, tienen el deber de salvaguardar a los niños, niñas y adolescentes, capacitando a los responsables de estos, para que proporcionen a los menores conocimiento de cómo deben de usar adecuadamente sus datos personales en las redes sociales e internet (Ley 1581, 2012).

Indicador # 7. Registro de las actividades de tratamiento

Estados Unidos

En el aparte relativo a la política de privacidad, del artículo 2 del consumer privacy act de California, se establece como un derecho del titular de la información, requerir información sobre las categorías de datos personales que ha recopilado la empresa durante los últimos 12 meses, identificación de las fuentes de las que provienen los datos recogidos, información del propósito comercial para la recolección o venta de información, al igual que la indicación de las categorías de datos que la empresa ha vendido, si lo hizo, y la categoría de a quienes vendió dichos datos durante los últimos 12 meses. Es por esto que, aunque no se indique de manera expresa la obligación de guardar registro de las actividades de tratamiento, para cumplir con las obligaciones indicadas anteriormente, la empresa debe hacerlo (Ley de privacidad del consumidor de California, 2018).

China

En China, el artículo de 41, inciso 1, de la ley de Ciberseguridad china, establece que los operadores de red, al utilizar información personal, como lo es el tratamiento de la misma, debe expresar el propósito, método y alcance del uso que se dará a los datos personales recopilados. Aun y cuando este artículo establece la obligación de expresar el método y alcance del uso de la información, no establece la obligación de guardar un registro de las actividades de tratamiento que se realizaron sobre los datos, así como tampoco lo establece la ley en mención (Ley de Ciberseguridad China, 2017).

España

Por su parte, España regula este tema al establecer que cuando se obtengan los datos personales directamente de su titular, el responsable, en cumplimiento del deber de información, debe indicar el responsable del tratamiento, la finalidad del mismo y la posibilidad del ejercicio de los derechos relativos al tema, indicando si los datos serán tratados para la elaboración de perfiles. Cuando los datos no son obtenidos directamente de su titular, el responsable debe indicar las categorías de datos objeto de tratamiento y las fuentes de las que extrajeron los datos.

Así mismo, la mencionada ley, en su artículo 31, numeral 1, establece que los responsable y encargados del tratamiento, deben guardar registro de las actividades de tratamiento indicadas en el artículo 30 del Reglamento General de Protección de Datos europeo, el cual indica que se debe guardar registro, de la indicación del responsable del tratamiento, los fines del tratamiento, la indicación de a quienes se les comunicaron los datos, entre otros. Mencionando en el mismo artículo, en su numeral cuarto, que el registro guardado deberá ser puesto por parte del responsable a disposición de la autoridad de control que lo solicite (Ley Orgánica de Protección de Datos de España, 2018).

Brasil

El artículo 6, numeral 4, de la ley de datos personales brasileña, establece dentro de su principio de acceso gratuito, la posibilidad del titular de los datos personales de consultar la forma y duración del tratamiento de los datos, al igual que la integridad de los mismos. El mismo artículo, en el numeral 6, establece el principio de transparencia y dice que, se les debe garantizar a los titulares de los datos, información clara, precisa y de fácil acceso, respecto al desempeño del tratamiento y los agentes que intervinieron en este. Así mismo, el numeral 10 de dicho artículo, establece una rendición de cuentas por parte del responsable del tratamiento, de la adopción de medidas para la observancia y el cumplimiento de las normas de protección de datos personales.

La misma ley, en su artículo 9, establece el derecho del titular de los datos a la información del tratamiento que sobre los mismos se ha efectuado, estableciendo una serie de requisitos que debe cumplir el informe de dicho tratamiento, entre los que se encuentran la indicación del propósito del tratamiento, su forma y duración, sus responsables, información sobre el uso compartido de datos y el propósito, entre otros (Ley General de Protección de Datos Personales de Brasil, 2020).

Colombia

La ley 1581 de 2012, en su artículo 8 literal a, establece el derecho del titular de los datos a conocer la información que sobre este se tiene, y el literal c, el derecho a ser informado bien sea por el responsable o por el encargado del tratamiento, respecto del uso que se les ha dado a los datos personales que sobre la persona se han recogido, si así lo solicita (Ley 1581, 2012).

Así mismo, el decreto 1377 del 2013 en su artículo 4, inciso 2, establece que, a solicitud de la Superintendencia de Industria y Comercio, el responsable del tratamiento debe indicar los procedimientos que se usaron para la recolección de los datos, almacenamiento, uso y circulación de la información recolectada, al igual que la expresión de las finalidades de su recolección y una explicación de la necesidad de recolección de los mismos. Siendo de igual manera consagrado por el artículo 11 del mismo decreto que, los responsables y encargados del tratamiento deben documentar los procedimientos que llevan a cabo para el tratamiento (Decreto 1377, 2013).

Indicador # 8. Seguridad de los datos personales

Estados Unidos

En el consumer privacy act de California, no se establece la obligación de adoptar medidas tendientes a garantizar la seguridad de los datos personales, así como tampoco a evitar su acceso sin autorización.

China

A lo largo de la ley de Ciberseguridad china se hace múltiples menciones a la seguridad de la red, siendo esta tratada en gran parte de sus artículos y convirtiéndose en un eje central de su regulación. Dicha legislación establece en múltiples apartados la obligación de mantener la seguridad en la red por parte de aquellos agentes que intervienen en esta. Se establece de igual manera un capítulo para regular la seguridad de la información en la red, siendo este, el capítulo 4, el cual va desde el artículo 40 hasta el artículo 50. En el artículo 42, inciso 2, de dicho capítulo se establece la obligación de tomar medidas técnicas, además de aquellas que resulten necesarias para garantizar la seguridad de la información. Así como de tomar medidas correctivas en caso de vulneración y avisar a tiempo tanto al titular de la información como a la autoridad competente la ocurrencia de esta (Ley de Ciberseguridad China, 2017).

España

El artículo 28 de la ley orgánica de protección de datos española, remite a los artículos 25 del reglamento general de protección de datos europeo, el cual establece en el numeral 2 que, el responsable del tratamiento debe aplicar medidas técnicas y organizativas tendientes a garantizar que los datos no sea accesibles sin autorización. Siendo esta la única disposición que se puede encontrar en la ley orgánica de protección de datos española sobre la obligación de adoptar medidas que garanticen la seguridad de los datos. Así mismo el artículo 82 de la ley española establece el derecho a la seguridad de las comunicaciones que se trasmiten por medio del internet (Ley Orgánica de Protección de Datos de España, 2018).

Brasil

En Brasil, la ley general de protección de datos regula el aspecto de la seguridad de los datos en el capítulo 7, relativo a la seguridad y buenas prácticas, en el cual se establece en su artículo 46, medidas tanto técnicas como administrativas para garantizar la seguridad de la información por parte del responsable del tratamiento y posibilita a la autoridad nacional en la materia a establecer normas técnicas mínimas. En el artículo 47 se ordena a todo el que intervenga en cualquier fase del tratamiento, garantizar la seguridad de la información y en el artículo 48 se impone la obligación al controlador de informar tanto a la autoridad nacional como al titular de los datos en caso de vulneraciones a la seguridad que puedan causar daños (Ley General de Protección de Datos Personales de Brasil, 2020).

Colombia

La ley 1581 de 2012, en su artículo 4, el cual regula los principios del tratamiento de datos, establece en su literal g el principio de seguridad, según el cual, la información sujeta a tratamiento debe ser manejada teniendo en cuenta la adopción de medidas técnicas, humanas y administrativas

que permitan garantizar la seguridad de la información, entre otras cosas, del acceso sin autorización. Así mismo, la ley en mención, en el artículo 17, literal e, impone el deber al responsable del tratamiento de conservar la información bajo medidas de seguridad que garanticen su integridad, imponiéndole igualmente, en el literal i, del mismo artículo, el deber de exigir del encargado del tratamiento, el mantenimiento de las condiciones de seguridad y en el literal n el deber de informar las violaciones a los códigos de seguridad que se lleguen a presentar, a la autoridad encargada de la protección de los datos. Siendo los deberes establecidos en los literales e y n, del artículo antes mencionado, aplicables también a los encargados del tratamiento, según el artículo 18 (Ley 1581, 2012).

Por su parte, el Decreto 1377 de 2013 establece en su artículo 19 la adopción de medidas de seguridad, siendo estas medidas instrucciones que imparte la superintendencia de industria y comercio colombiana con el fin de garantizar la seguridad en el tratamiento de los datos personales (Decreto 1377, 2013).

Indicador # 9. Sanciones pecuniarias en caso de violación a datos personales

Régimen Sancionador

Estados Unidos

En Estados Unidos no se encuentra regulado las sanciones o régimen sancionador por la violación a los datos personales en la Ley estudiada California Consumer Privacy Act, sin embargo, en el Código Civil de California (AB-375), en su División 3 sobre las obligaciones, parte 4, TÍTULO 1.81.5, en su sección 1798.150 y 1798.155, Se encuentra todo lo relacionado con las sanciones derivadas de la violación de los datos personales de los consumidores en California. Como sanciones imponen para restablecer los daños ocasionados un monto no mayor de $750 dólares por daños, medidas cautelares o cualquier otra que el tribunal considere. Si la entidad que se notificó por la vulneración a algún derecho, si no subsana dentro de los 30 días siguientes será sometido a otras sanciones pecuniarias de hasta $2.500 dólares o $7.500 si fuese intencional (Código Civil de California, 1872).

China

En cuanto a la República Popular China, el Gobierno toma medidas de vigilancia y control para la detección de violaciones o prácticas contrarias a la ley respecto de la protección de datos personales y su debido tratamiento, también para evitar amenazas de posibles ataques, interferencias o destrucciones a los datos personales de este país, la regulación de la protección de datos personales está contenida en la Ley de Ciberseguridad China y sus sanciones desde el artículo 59 al 74.

Cualquier operador de la red, tiene la obligación de brindar seguridad idónea y suficiente que cumpla con los estándares de protección del Estado Chino que sean suficientes para ese fin, implementando procedimientos operativos y medidas técnicas que sirva como garantía de seguridad de los datos y la red cibernética, pues de lo contrario el encargado debe de seguir las

disposiciones legales de notificar tanto a los titulares de los datos como a los órganos de control encargados de la vigilancia de la seguridad en el ciberespacio en el país para detener el daño o riesgo.

Respecto de las sanciones, China tiene un marco amplio de multas pecuniarias, sancionando a toda persona natural o jurídica que no cumpla con los requisitos de seguridad en la red para evitar posibles accidentes y no poner en riesgo la seguridad nacional ni alterar el orden público. El incumplimiento de estas obligaciones puede generar una multa de hasta 500.000 yuanes como el máximo de multas y 5.000 yuanes el mínimo. Las conductas más multadas por este país son aquellas en las que los operadores de la red u organizaciones sean parte de actividades que conlleven a fraude, actuaciones criminales, enajenaciones en la red de objetos ilícitos, la invasión de la red de otras personas, el hurto de los datos, el interferir con el funcionamiento normal de la red poniendo en riesgo la seguridad nacional, serán multadas con hasta 500.000 yuanes siendo la multa más alta a imponer (Ley de Ciberseguridad China, 2017).

España

En cuanto a las sanciones en caso de violación de datos personales, en España se ha desarrollado ampliamente basando su régimen sancionador en sanciones y medidas correctivas que se encuentra contenidas en el artículo 76 de la de protección de datos española. El Gobierno Español, a través de la mencionada ley desarrolla en su contenido en este aspecto el Reglamento (UE) 2016/679 del parlamento europeo y del consejo de la Unión Europea, en cuál basa totalmente los medidores de las sanciones pecuniarias que en España debido a la sanción que por la violación de los datos personales le son aplicables. En tal Reglamento Europeo en su Art 83 despliega todo lo concerniente a los medidores sobre los cuales establece las sanciones por la vulneración de datos personales, que son desarrolladas según la gravedad de la infracción y el sujeto infractor de los datos personales, el carácter continuado de la infracción, entre otros.

Las multas serán de 10 000 000 EUR como máximo, si se trata de la violación de los datos personales por parte del responsable y encargado, organismo de certificación o la autoridad de control y que infrinjan los derechos tales como los de los menores, o la respuesta tardía a la violación de datos personales entre otras disposiciones que salvaguardan las garantías pertinentes en este tema. Será de 20 000 000 EUR como máximo cuando se violaren los principios del tratamiento en relación con la licitud de este y forma de obtención del consentimiento para el trato de los datos, que se violen derechos de los interesados en relación a la transparencia del uso de los mismos para con el titular, los principios en relación a la transferencia de los datos personales, entre otros; por último, será multa del mismo valor anterior a quien contraríe las resoluciones del órgano de control sobre protección de datos personales (Ley Orgánica de Protección de Datos de España, 2018).

Brasil

En este aspecto, Brasil en su Régimen Sancionatorio tiene diversas penalidades por la violación a los datos personales, dejando la sanción pecuniaria como las más graves. Este régimen se encuentra estipulado en la Ley Federal 13.709/18 de Brasil en su artículo 52 desplegando cada sanción según

el grado de gravedad de la conducta. La violación a aspectos como la privacidad, la intimidad, el honor, la imagen, la dignidad o incluso poner en riesgo la seguridad nacional, puede ser motivo de hasta ser suspendido del ejercicio de la actividad de procesamiento de los datos personales.

Las sanciones son llevadas a cabo para que se cumplan las garantías legales del afectado, lo cual se da lugar a que los entes de control se cercioren que el caso sujeto a investigación este cubierto de seriedad, que se pueda identificar las infracciones invocadas y los derechos lesionados y hacer cumplir tanto los derechos del titular como del infractor. En el desarrollo de las sanciones como primero está la advertencia que es un tiempo que se da para adoptar las medidas correctivas por la infracción cometida, por consiguiente se encuentra establecidas las multas, que serán la multa simple con hasta cincuenta millones reales R $ 50,000,000.00 por cada violación a la ley; por consiguiente está la multa diaria, que su monto límite es el mismo al ya mencionado, entre otras sanciones como la publicación de la infracción, bloqueo o eliminación de los datos violentados (Ley General de Protección de Datos Personales de Brasil, 2020).

Colombia

En Colombia el ámbito sancionatorio por violación de datos personales se encuentra en la Ley 1581/2012 Habeas Data en su capítulo II, artículo 22. Esta última sanciona las condutas como el acceso no autorizado de los datos, la adulteración de estos, la pérdida y el no respetar las condiciones de seguridad y privacidad, sobre todo si se trata de datos sensibles que son los datos más delicados para la integridad de una persona física del Estado Colombiano. Se impondrán multas de hasta 2.000 SMLMV y será acumulable mientras perdure la infracción. También podrá imponerse la suspensión de las actividades de tratamiento de los datos hasta por 6 meses; teniendo como criterio gradual de la sanción varios aspectos como la medición del daño o peligro causado tales como, el provecho económico obtenido ilícitamente por la violación, la reiteración de tal conducta entre otros agravantes que permiten estudiar el caso en concreto e imponer una sanción justificada.

Para el ejercicio de las Autoridades de control y vigilancia en Colombia, se cuenta con un solo despacho incluido dentro de la organización de la Superintendencia de Industria y Comercio para atender todas las vulneraciones a los datos personales del país y únicamente en el ámbito privado, pues en el ámbito público, se debe remitirse a la Procuraduría General de la Nación para que el caso sea atendido (Ley 1581, 2012).

Indicador # 10. Existencias de un órgano de control y vigilancia de los datos personales

Estados Unidos

En Estados Unidos, para la vigilancia y control del cumplimiento de la Ley California Consumer Privacy Act (CCPA) cuentan con la Comisión Federal de Comercio (FTC). Este es un órgano independiente que se encarga de contrarrestar la competencia desleal en Estados Unidos como otras tareas varias de control que se le ha asignado como la protección a las prácticas de compra y venta de datos personales, ya que ésta práctica es permitida en este país. Desde su creación, el

Congreso promulgó algunas leyes que las puso bajo su vigilancia otorgándole más autoridad en este ámbito.

China

Por parte de China, cuenta con un departamento de información de la red nacional que será el ente encargado de vigilar y dirigir el funcionamiento de rastreo y monitoreo de la red e internet para mitigar los riesgos y vulneraciones. Así como también se complementa con otros órganos como el departamento de telecomunicaciones del Consejo de Estado Chino, el departamento de seguridad publica entre otros que sirven de apoyo a la vigilancia de la red cibernética que consta en el artículo 8 de la Ley de Ciberseguridad

El sistema de monitoreo de seguridad de red en china es creado por el Estado para que por medio del departamento de información de la red nacional se coordine todas las disposiciones legales sobre el tratamiento y protección de los datos, mejorando el monitoreo de seguridad en la web, mejorar la evaluación de riesgos para tomar nuevas medidas o planes de emergencia para accidentes de seguridad de la red.

A los posibles peligros de seguridad cibernética, el gobierno chino en el artículo 54 dispone medidas que deben implementar los órganos competentes de la vigilancia como recopilar e informar de manera oportuna los posibles riesgos en la seguridad para su ampliación, recaudar personal capacitado y profesional para la revisión de información sobre riesgos de seguridad en la web, divulgar alertas y medidas a la sociedad para fomentar conciencia de autocuidado en el ciudadano con la seguridad de su información.

Las emergencias ocurridas por violación a la seguridad cibernética, será iniciada el plan de emergencia de incidente de la seguridad de la red para su evaluación y estudio para exigir a los involucrados, medidas necesarias para suprimir los riesgos o daños (Ley de Ciberseguridad China, 2017).

España

En España por su parte, cuenta con la Agencia Española de Protección de Datos encargada de la vigilancia y monitoreo de los datos personales en la web según lo establecido en el Título VII, Capítulo I, artículo 44 de la ley de protección de datos de este país, tendiendo el respaldo de las administración pública, la tributaria y de la seguridad social para remitir toda la información pertinente para que la Agencia Española de Protección de Datos pueda llevar a cabo actividades de investigación, siempre y cuando exista la necesidad de la remisión de dicha información como informes y antecedentes de las personas, una de esas necesidades es que se esté identificando al infractor de la ley y el reglamento de protección de datos.

La AEPD es competente para inspeccionar y solicitar informes con el fin de evaluar el tratamiento e inspeccionar los equipos utilizados para ello para mitigar posibles vulneraciones a los datos y desarrollar proyectos de prevención de violaciones (Ley Orgánica de Protección de Datos de España, 2018).

Brasil

En Brasil, el órgano competente encargado del control y vigilancia de la protección de los datos personales es la Autoridad Nacional de Protección de Datos (ANPD) como consta en el artículo 55 de la Ley Federal 13.709/18, siendo este un órgano de administración nacional encargado de supervisar, implementar medidas, garantizar y supervisar la seguridad de los datos personales en las redes y el cumplimiento de la ley brasileña sobre la protección de datos.

La ANPD es competente para solicitar a cualquier operador de las redes un informe sobre el estado de protección de los datos a que tiene acceso del cual podrá emitir una opinión e implementar medidas de protección como asistencia técnica complementaria, así como establecer normas que complementen la protección de los datos.

Colombia

En Colombia se tiene como ente de control y vigilancia de los datos personales la Superintendencia de Industria y Comercio cuando se trata de datos de personas privadas, cuando se trata en el ámbito público, será la Procuraduría General de la Nación la competente para tratar las posibles vulneraciones de los datos personales. Como tal no cuenta con un órgano independiente de monitoreo y rastreo en la red y el internet para recopilar las infracciones y violaciones de derechos por el tratamiento indebido de los datos personales.

Los órganos de vigilancia en Colombia son encargados de promover y adelantar investigaciones cuando se desconozca el derecho al habeas data, debe promover instrucciones sobre las medidas de seguridad a proyectar por los responsables, también promocionar la existencia de los derechos de protección de datos a todas las personas y capacitar y mantener informado a los ciudadanos sobre cómo proteger sus datos, así como también administrar las bases de datos del Registro Nacional Publico.

Capitulo III. Análisis de resultados: comparación de las legislaciones sobre protección de datos personales

La comparación de la legislación en materia de protección de datos, se realizó teniendo en cuenta los siguientes criterios de selección: Estados Unidos, por ser el país donde se han creado varias de las más grandes compañías tecnológicas en el mundo; China, debido a que es uno de los países con mayor crecimiento en el sector tecnológico; España, dado que su ley se basa en el reglamento general de protección de datos europeo, normativa que ha sido referente global en la materia, nos permite entender parte de esta, además de la propia española que es una de las más sólidas; Brasil, se trata uno de los países que más está avanzando en el sector tecnológico en Suramérica, siendo uno de los países escogido por la empresa española Telefónica para realizar pruebas de la tecnología Open Ram 4G Y 5G; y Colombia, debido a que se han creado en el país centros de excelencia y apropiación –CEA´s, buscando posicionar a Colombia como referente en Big Data Analytics.

A continuación, se presentará un cuadro donde se indican las normas donde se pueden observar las diferencias, además, desde la selección y desarrollo de los indicadores se evaluarán cualitativamente, en una escala de: suficiente, en caso de ofrecer una protección optima de los datos personales; aceptable, en caso de que su protección no sea optima, pero tampoco deficiente; e insuficiente, en caso de que su nivel de protección sea insuficiente en relación con el indicador y los demás países.

Cuadro comparativo

Tabla 3 Cuadro comparativo, legislaciones (EEUU, China, España, Brasil, Colombia)

Cuadro Comparativo							
Numero de Indicador	Nombre del indicador	Descripción del Indicador	Legislación EEUU	Legislación China	Legislación Europa	Legislación Brasil	Legislación Colombia
1	**Existencia de una ley unificadora de la legislación sobre datos personales**	Que exista una ley unificada sobre datos personales y no una regulación dispersa	NO	SI	SI	SI	SI
2	**Obligación de indicar con qué fin se recoge la información para el tratamiento (Derecho de información en el tratamiento de datos)**	Para la recolección de los datos se debe informar con que fines se hace y con que fines serán tratados estos posteriormente	SI	SI	SI	SI	SI

3	**Limitación del uso y tratamiento de los datos personales recolectados**	Que los datos recolectados sean únicamente utilizados para aquellos fines que fueron informados (y que su recolección sea necesaria para la actividad	SI	SI	SI	SI	SI
4	**Posibilidad de eliminación de los datos**	Posibilidad por parte del titular de los datos de exigir la eliminación de estos de la base de datos en la que se contienen	SI	SI	SI	SI	SI
5	**Transferencia a terceros sin consentimiento del titular y transferencia internacional**	Que se deba contar con el consentimiento del titular de los datos para cualquier tipo de transferencia a terceros de los mismos	SI	SI	SI	SI	SI
6	**Protección especial de los datos de los niños, niñas y adolescentes**	Que la legislación prevea una protección especial para los datos de los niños, niñas y adolescentes	SI	SI	NO	NO	NO
7	**Registro de las actividades de tratamiento**	Los encargados del tratamiento de los datos deben guardar el registro de las actividades de tratamiento que realizaron	SI	SI	SI	SI	SI
8	**Seguridad de los datos**	Que se establezcan medidas tendientes a asegurar la seguridad de los datos de la intromisión de terceros sin autorización	NO	SI	SI	SI	SI
9	**Sanciones pecuniarias en caso de violación a datos personales**	Que se establezcan sanciones pecuniarias en caso de violación de las disposiciones sobre datos personales	NO	SI	SI	SI	SI
10	**Existencias de un órgano de control y vigilancia de los datos personales**	Que exista un órgano encarga del control y vigilancia del cumplimiento de las disposiciones sobre datos personales	SI	SI	SI	SI	SI

Indicador # 1. Existencia de una ley unificadora de la legislación sobre datos personales

Tabla 4 Medición cualitativa

Medición Cualitativa	
EE.UU	INSUFICIENTE
CHINA	SUFICIENTE
ESPAÑA	SUFICIENTE
BRASIL	SUFICIENTE
COLOMBIA	ACEPTABLE

Estados Unidos no cuenta con una legislación nacional en materia de protección de datos personales, siendo este tema regulado de manera autónoma por cada uno de sus estados. La ley más completa en la materia en el país norteamericano corresponde a la Ley de Privacidad del Consumidor de California, pero la misma solo rige para el estado de California y no es de aplicación nacional, por lo que, en este punto, Estados Unidos brinda una protección insuficiente al no contar con una legislación nacional en la materia.

China cuenta con una ley de protección de datos personales de carácter nacional, se trata de la Ley de Ciberseguridad China, la cual no regula exclusivamente este tema, sino que regula una variedad de temas relacionados con el ciberespacio, entre los que cuenta con un espacio vital la protección de datos personales. Por esta razón China, al contar con una legislación nacional y unificada en el tema dedicada exclusivamente al ámbito de la red, brinda una protección suficiente a los ojos de este indicador.

Por su parte, España regula este aspecto en la Ley Orgánica de Protección de Datos, la cual fue expedida con el fin de acoplarse a la regulación europea en la materia. Se trata de una ley de carácter nacional, la cual rige en todo el territorio español, y unifica la legislación en la materia, brindando así España una protección suficiente en este aspecto.

Brasil igualmente cuenta con la legislación nacional, la cual rige en todo su territorio y unifica la regulación de la protección de datos personales. Esta ley es la Ley General de Protección de Datos, bajo la cual se cumple de manera suficiente con el criterio evaluativo de este indicador.

A su vez, Colombia regula la protección de datos personales a través de la Ley 1581 de 2012, la cual fue reglamentada por el Decreto 1377 del 2013, rigiendo ambos en todo el territorio nacional y siendo la legislación reguladora de la materia. Por esto, aunque Colombia cuente con una legislación de carácter nacional, no cuenta con una completa unificación en el tema, al existir una ley que es reglamentada por un decreto, razón por la cual bajo a la luz del presente indicador, su protección es aceptable.

Indicador # 2. Obligación de indicar con qué fin se recoge la información para el tratamiento

Tabla 5 Medición cualitativa

Medición Cualitativa

EE.UU	SUFICIENTE
CHINA	SUFICIENTE
ESPAÑA	SUFICIENTE
BRASIL	ACEPTABLE
COLOMBIA	SUFICIENTE

El estado de California, Estados Unidos, brinda una protección suficiente en este punto, al establecer la obligación por parte de quien recolectará los datos, de dar aviso de la categoría de datos que recolectará y los fines que se le dará a los mismos.

En lo que respecta a China, su legislación igualmente da suficiente protección bajo este indicador, estableciendo la obligación de informar tanto el alcance como el fin de la recolección de los datos personales, y ligando estos a diversos principios y a la obtención del consentimiento por parte del titular de los datos.

España supedita la recolección de los datos y tratamiento de los datos personales a que se obtenga el consentimiento libre, especifico, informado e inequívoco por parte del titular de los datos, estableciendo igualmente, al momento de la recolección de los mismos, la obligación de informar la finalidad con que serán tratados y si es para una pluralidad de fines debe constar de manera expresa e inequívoca que es para todos estos. Por esto, brinda una protección suficiente a los ojos del presente indicador.

A su vez, en Brasil, se establece la obligación para el tratamiento de los datos personales de obtener el consentimiento del titular, mismo que debe referirse a fines específicos, pues en caso de autorizaciones genéricas para el tratamiento son nulas. El tratamiento se encuentra supeditado a lo consentido por el titular de los datos. Este país no establece de manera expresa en su articulado la obligación de informar que datos serán recolectados, por lo que, a pesar de establecer la obligación de indicar los fines del tratamiento, su protección a la luz de este indicador es aceptable.

En Colombia, su legislación establece la obligación de que, a más tardar al momento de recolectar los datos personales, se informe a su titular sobre qué datos serán recolectados, al igual que la finalidad con la que serán tratados los mismos, obligación que reitera en varios de sus artículos. Bajo este entendido, Colombia, al establecer la obligación de indicar los datos que serán recolectados y la finalidad con que serán tratados los mismos, brinda un nivel de protección suficiente en este aspecto.

Indicador # 3. Limitación del uso y tratamiento de los datos personales recolectados

Tabla 6 Medición cualitativa

Medición Cualitativa	
EE.UU	INSUFICIENTE
CHINA	SUFICIENTE
ESPAÑA	SUFICIENTE

BRASIL	SUFICIENTE
COLOMBIA	SUFICIENTE

En Estados Unidos, específicamente en la ley de privacidad del consumidor de California, no se encuentra ningún tipo de disposición que de manera expresa limite la recolección de los datos personales a aquellos indispensables para el objeto del contrato, así como tampoco ninguna que limite el uso a los fines indicados al momento de su recolección. Siendo así que en este ítem Estados Unidos ofrece una protección insuficiente.

En China se establece la obligación de supeditar el tratamiento de los datos personales recolectados, al acuerdo al que a la hora de la recolección se llegó con el titular de los mismos, la cual debió estar limitada a la necesaria para la prestación del servicio, lo cual es reiterado en otro de sus artículos con la prohibición de recolectar información que no esté relacionada con el servicio que se presta, lo cual ligan a distintos principios del tratamiento de datos.

La legislación española establece que el tratamiento de los datos personales debe estar basado en el consentimiento que previamente el titular de los mismos había dado, supeditándose a los fines en aquel momento consentidos. De la misma manera establece que la prestación del servicio no puede ser supeditada a que se consienta el tratamiento de los datos para fines que no son necesarios para el objeto de contrato. Brindando así una protección suficiente en este aspecto.

Brasil, por su parte, en sus principios para el procesamiento de datos personales, establece que el tratamiento debe ser compatible con los fines que se le informaron al titular de los datos, prohibiendo cualquier tratamiento distinto de aquel para el cual se recolectaron y limitando el procesamiento de los mismos, a los estrictamente necesarios para cumplir el fin previsto. Por lo cual, en lo que a este indicador respecta, ofrece una protección suficiente.

La legislación colombiana, a su vez, establece que la recolección de datos personales debe limitarse a aquellos que sean adecuados y guarden pertinencia con los fines para los cuales se recolectan y limita su uso a aquellos fines que justificaron su recolección. Con lo cual brinda una protección suficiente en este aspecto.

Indicador # 4. Posibilidad de eliminación de los datos personales

Tabla 7 Medición cualitativa

Medición Cualitativa	
EE.UU	INSUFICIENTE
CHINA	ACEPTABLE
ESPAÑA	SUFICIENTE
BRASIL	INSUFICIENTE
COLOMBIA	SUFICIENTE

Por parte de Estados Unidos, la eliminación de los datos personales es posible y se encuentra regulada en la Ley California Consumer Privacy Act, en la cual, tal actuación está inmersa bajo ciertos procedimientos, de los cuales el titular de los datos personales está en el deber de transmitir

una solicitud a la entidad que está tratando y comercializando sus datos y adicional a esta solicitud, posteriormente debe de elaborar una segunda manifestación expresa de voluntad solicitando que sus datos sean eliminados de toda base de datos sometida a tratamiento y venta; por otro lado la solicitud en mención debe de cumplir con unos requisitos establecidos por la empresa, que si no son llevados bajo esos parámetros la empresa prestará orientación de cómo hacerlo en debida forma. Lo anterior implica que el titular de los datos personales sea sometido a un procedimiento que se puede tornar dilatorio, pues tanto el derecho a la protección de datos personales como la eliminación de estos, son un derecho personalísimo que entraña solamente al interés personal del titular, por lo cual bastaría la sola voluntad de que sus datos sean eliminados desde la primera oportunidad. En este orden de ideas Estados Unidos tiene un nivel intermedio de protección en garantía a la eliminación de los datos personales contenidas en bases de datos digitales en redes sociales e internet.

En China, la eliminación de los datos personales está mencionada en algunos artículos, sin embargo, no está desarrollada ampliamente; para llevar a cabo la eliminación de los datos personales es posible solicitar al operador responsable y encargado que lo haga, el titular podrá solicitarlo también en el momento que detecte alguna vulneración o practica maliciosa a sus datos personales y no podrá en cualquier momento. Por lo anterior, China se encuentra en un nivel aceptable de protección en relación con este indicador.

En España por su parte, contempla la supresión de los datos personales únicamente en lo contenido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea y no en su ley nacional, el cual denomina también a tal actuación como el Derecho al Olvido; en el momento que el titular de los datos solicite la eliminación de estos, sin dilación alguna indebida según el artículo 17 #1 se remitirá inmediatamente a la supresión. Lo que otorga diligencia e inmediatez a la atención y ejecución de este derecho que es lo que todo titular espera con sus datos personales. España se encuentra, por lo anterior en un nivel suficiente de protección da los datos concernientes a su eliminación, a pesar de dejar a suerte del reglamento su protección y no lo desarrolla internamente en su país adecuándolo a las particularidades del mismo.

Por parte de Brasil, desarrolla este derecho en tres artículos de forma dispersa en la ley, los cuales permiten la eliminación de los datos personales una vez se haya culminado con el tratamiento o manipulación al que fueron sometidos. El Gobierno Brasileño permite que los datos personales recolectados se conserven si los han sometido a anonimato, las empresas podrán usar e investigar con esos datos personales. Brasil se encuentra en un nivel bajo de protección, pues no especifica a fondo los derechos que tienen las personas a que sus datos sean eliminados en cualquier momento y el deber que tienen todos los operadores de red de mantener informado a los titulares. La posibilidad de conservar no permite a cabalidad una eliminación completa de los datos. Lo que conlleva a que Brasil esté en un nivel insuficiente respecto a este indicador.

Colombia, también regula la eliminación muy someramente en algunos artículos a lo largo de la Ley Habeas Data y se complementa con el Decreto 1377/2013, el cual el titular de los datos personales podrá en cualquier momento solicitar la supresión de los datos, entre otras razones por haber infracciones frente al uso y tratamiento de los datos y cuando se desconozcan las garantías

legales y constitucionales de la Ley de protección de datos. Colombia tiene un grado de protección suficiente frente a la protección de este derecho.

Indicador # 5. Transferencia Internacional y Transferencia a terceros de los datos personales

Tabla 8 Medición cualitativa

Medición Cualitativa	
EE.UU	INSUFICIENTE
CHINA	SUFICIENTE
ESPAÑA	SUFICIENTE
BRASIL	SUFICIENTE
COLOMBIA	SUFICIENTE

En Estados Unidos la transferencia internacional de los datos personales es permitida, la misma, según la Ley California Consumer Privacy Act (CCPA) es denominada como la divulgación o venta de la información personal, es decir, que en Estados Unidos la compra y venta de los datos personales es una práctica normal que permite a las empresas recopilar datos de sus usuarios para el uso y tratamiento de los mismos para evaluar cierta información de interés de la misma empresa. Lo anterior permite determinar que la seguridad en la transferencia de los datos personales a terceros no es tan bien regulada en comparación con los otros países como China.

En China, la transferencia internacional de datos es muy proteccionista, pues todos los datos personales recopilados serán almacenados solo en el territorio nacional, si no hay una razón o mandato legal que justifique la transferencia a terceros países no será permitido y tal hecho será sancionado con hasta 100.000 yuanes, entre otras sanciones por contrariar esta disposición. Esto permite que China tenga un alto grado de protección frente a la trasferencia internacional de los datos que son compilados en redes sociales e internet en el país.

En España, es coherente la forma como han regulado la transferencia internacional de datos personales, pues si bien está desarrollada en la ley nacional que lo regula considerablemente, es complementada con el Reglamento (UE) Del Parlamento y del Consejo sobre protección de datos personales, que también es regulado allí de forma amplia y lo que es aún más importante y por esto España cumple con una protección suficiente en este aspecto, por la razón de que aplica tal Reglamento a todos los Estados parte de la Unión Europea, que permite que la transferencia internacional de los datos personales en internet sea segura entre los Estados, pues para llevarse a cabo, cada uno debe de cumplir con un estándar de protección óptimo y el mismo será verificado por cada país antes de acordar la transferencia entre sí. Por lo anterior, España tiene un alto grado de protección frente a este derecho.

Por otra parte, Brasil protege la transferencia internacional de datos con varias condiciones importantes para esta actividad, como lo es contar con clausulados contractuales para la transferencia con países a donde se destinarán los datos y que estos cuenten con una buena

protección de los mismos en internet, esto permite que haya un vínculo entre estados que determine el conjunto de derechos y obligaciones de protección que aplica a los países que contraten para la transferencia internacional de los datos, lo cual el Estado Brasileño evaluará en debida forma, pues si no se cuenta con lo anterior no será posible tal diligencia si no es sumamente necesario.

A su vez, en Colombia también es obligatorio para la transferencia internacional tener un contrato de transmisión en donde conste que el país destino cuenta con una igual o mayor protección de los datos personales en redes sociales e internet, de otra forma no sería posible llevar a cabo transferencia alguna si no hay consentimiento para ello. Está en cabeza del Superintendente de la Superintendencia de Industria y comercio facultar la transferencia en los casos que no están previstos como excepciones a la prohibición de la transferencia, según el artículo 26 PAR 1º. Debido a lo anterior Colombia otorga una protección suficiente para la transferencia internacional de los datos personales.

Indicador # 6. Protección de niños, niñas y adolescentes en internet

Tabla 9 Medición cualitativa

Medición Cualitativa	
EE.UU	SUFICIENTE
CHINA	ACEPTABLE
ESPAÑA	INSUFICIENTE
BRASIL	ACEPTABLE
COLOMBIA	INSUFICIENTE

La protección de los datos personales de niños, niñas y adolescentes en Estados Unidos cuenta con una ley independiente dedicada exclusivamente a la protección de los datos de los menores en internet, así mismo, China ha empleado una ley individual dirigida a los menores de edad aparte de la general sobre protección de datos como la Ley de ciberseguridad o la Ley de California por parte de Estados Unidos.

Estados Unidos exige al operador de internet que cuente con el consentimiento del tutor del menor y que éste último sea verificable, es decir, como se mencionó con anterioridad al respecto, el consentimiento verificable es la certeza de que la persona que firmó tal permiso si sea el padre o la madre del menor. Lo anterior, con el desarrollo de un método de obtención del consentimiento que, entre otras cosas puede contener la opción de llamada o videoconferencia para tal rectificación, como se explicó en el desarrollo de este indicador proporcionando una protección suficiente en relación con los datos de menores en internet.

Respecto de China si bien también hay una ley independiente que garantiza un buen grado de protección, la ley sobre la protección en línea de la información personal de menores no cuenta con un procedimiento de obtención del consentimiento tan estricto como el de Estados Unidos. Siendo así, en el desarrollo de dicha ley solo se garantiza un nivel de protección aceptable para los niños, niñas y adolescentes en el uso de las redes sociales e internet.

España por otro lado, no ha desarrollado una ley independiente que regule la protección de los datos del menor en internet, dedica un artículo a esta regulación en el cual lo hace de una forma muy general y no da un desarrollo a profundidad, por lo anterior, España tiene un nivel de protección insuficiente frente a este indicador.

Brasil, si bien regula este ámbito en varios artículos, no cuentan con una legislación tan sólida y minuciosa como las legislaciones de Estados Unidos y China. Aun así, se exige que se verifique el consentimiento del tutor o los padres del menor, mediante los medios tecnológicos a disposición. Por esta razón, Brasil tiene una calificación aceptable frente a la protección de este indicador.

Respecto de Colombia, en la Ley Habeas Data regula este ámbito en un solo artículo como fue descrito anteriormente. En este mismo no se permite el tratamiento de los datos si no es necesario. Debido a su casi nula relación de este aspecto, Colombia ofrece una protección insuficiente.

En este orden de ideas, Estados Unidos y China quedan en el grado más alto de protección de los datos personales de niños, niñas y adolescentes en internet, siendo Estados Unidos el más garantista y proteccionista para el menor en el uso de las redes sociales e internet.

Indicador # 7. Registro de las actividades de tratamiento

Tabla 10 Medición cualitativa

Medición Cualitativa	
EE.UU	ACEPTABLE
CHINA	INSUFICIENTE
ESPAÑA	SUFICIENTE
BRASIL	SUFICIENTE
COLOMBIA	SUFICIENTE

Estados Unidos, no consagra el deber de guardar registro de las actividades de tratamiento sobre los datos personales como una obligación de quien los recolecta, sino como un derecho del titular de los mismos, quien podrá solicitar cierta información sobre el tratamiento que se le ha dado a sus datos, pero estando la misma limitada solo a los últimos 12 meses, razón por la cual tienen un nivel aceptable de protección, pues si bien se infiere que quien hace uso de los datos personales debe guardar registro del tratamiento dado a estos, con el fin de darle acceso a esta información a su titular si así lo solicita, este registro se limita en el tiempo a los últimos 12 meses.

La legislación China, si bien prevé que al utilizar la información personal se debe expresar el propósito, el método a usar y el alcance, no consagra la obligación por parte de quienes tratan los datos personales de guardar un registro del tratamiento al cual someten esta información. Por lo que China cuenta con una protección insuficiente en este punto.

Por su parte, España, consagra la obligación expresa, tanto por parte del responsable como del encargado del tratamiento de los datos personales, de guardar un registro de las actividades de tratamiento que sobre los datos realicen, mismo que deberá ser puesto a disposición de la autoridad

competente que lo solicita, brindando así el país europeo una protección suficiente bajo la perspectiva de este indicador.

En Brasil, si bien no se establece de manera expresa como una obligación el deber de guardar registro de las actividades de tratamiento llevadas a cabo sobre los datos personales, se sobreentiende la misma cuando se le da derecho al titular de los datos a acceder, entre otras cosas, a la indicación del propósito del tratamiento, su forma, duración, y sus responsables. Siendo así que, para brindar el acceso a esta información al titular de los datos, deben mantener un registro de estas actividades, por lo que Brasil si bien no consagra este deber expresamente, de su normativa que puede extraer que está presente. Por esto el país suramericano brinda una protección suficiente en este aspecto.

Por último, Colombia, establece de manera expresa la obligación por parte, tanto del responsable como del encargado del tratamiento, de documentar los procedimientos que llevan a cabo para el tratamiento de los datos personales. Consagrando igualmente para su titular, el derecho de acceder a la información sobre el tratamiento de sus datos, información a la que también tendrá acceso el órgano de control en la materia, si así lo solicita. Dando así Colombia un nivel de protección suficiente en lo que a este indicador respecta.

Indicador # 8. Seguridad de los datos personales

Tabla 11 Medición cualitativa

Medición Cualitativa	
EE.UU	INSUFICIENTE
CHINA	SUFICIENTE
ESPAÑA	SUFICIENTE
BRASIL	SUFICIENTE
COLOMBIA	SUFICIENTE

En Estados Unidos, específicamente en la ley de privacidad del consumidor de California, no se establece ninguna obligación de garantizar la seguridad e integridad de los datos personales recolectados, así como tampoco establece la obligación de adoptar medidas que eviten el acceso a los mismos por parte de terceros sin autorización. Siendo así que, en este aspecto, Estados Unidos brinda una protección insuficiente para los datos personales.

China por su parte, presenta cierta solidez en la protección de este punto, reiterando en varios de sus artículos el deber de garantizar la seguridad, la cual es uno de los ejes centrales de su legislación. En esta se establece la obligación de garantizar la seguridad de la información, así como de tomar las medidas necesarias en caso de vulneración y dar aviso al titular de los datos cuando esta ocurra, garantizando de esta forma un nivel suficiente de protección.

La legislación española se remite al reglamento general de protección de datos europeo para regular este tema, estableciéndose en aquel que el responsable del tratamiento aplica las medidas técnicas y necesarias para garantizar que los datos no sean accesibles a terceros sin autorización.

Siendo su calificación suficiente al establecer la obligación de adoptar medidas que eviten accesos no autorizados a los datos personales del titular, así mismo está establecido en su propia ley el derecho a la seguridad a las comunicaciones en internet.

Brasil, a su vez, establece en su ley de protección de datos la obligación de todos los que intervienen en cualquier fase del tratamiento, de garantizar la seguridad de los datos personales, debiendo adoptar las medidas necesarias para esto y faculta a la autoridad nacional en la materia a establecer estándares técnicos mínimos de seguridad. Lo cual, aunado a la obligación de informar tanto al titular de los datos como a la autoridad nacional, las vulneraciones a la seguridad que pudiesen causar daño, garantiza una protección suficiente en este indicador.

En lo que respecta a Colombia, su legislación establece la seguridad como uno de los principios del tratamiento de datos personales, imponiendo la obligación de adoptar medidas que garanticen la seguridad de los datos, con el fin de garantizar su integridad y evitar el acceso de terceros no autorizados. Las instrucciones para la adopción de estas medidas son dadas por la autoridad nacional en la materia. Así mismo, se establece el deber de informar a dicha autoridad sobre las violaciones a los códigos de seguridad que se presenten, con lo que Colombia garantiza un nivel suficiente de protección en este ítem.

Indicador # 9. Sanciones en caso de violación a datos personales

Régimen Sancionador

Tabla 12 Medición cualitativa

Medición Cualitativa	
EE.UU	INSUFICIENTE
CHINA	SUFICIENTE
ESPAÑA	SUFICIENTE
BRASIL	SUFICIENTE
COLOMBIA	ACEPTABLE

En Estados Unidos, como se mencionó anteriormente, no se cuenta con un régimen sancionador propio en la Ley estudiada California Consumer Privacy Act, sin embargo, de manera supletiva, este régimen se encuentra regulado en el Código Civil de California en sus secciones 1798.150 y 1798.155 que refiere a que la empresa que trata los datos, debe de llevar a cabo acciones suficientes y prácticas de seguridad óptimas para garantizar una protección a los datos personales, de lo contrario se puede iniciar una acción civil para sancionar prácticas como la violación de sus datos personales como la divulgación de los mismos si no son subsanables al momento de hacer la declaración expresa del incumplimiento por parte del titular, para que le sean restablecidos sus derechos. Cualquier empresa o persona puede recibir orientación sobre el procedimiento para hacer efectivo el derecho de protección de los datos por parte del Fiscal General.

En el caso de China, hay una amplia regulación dirigida a las sanciones por infringir la Ley de Ciberseguridad, especificando cada actuación que es sancionable y su monto en yuanes de la sanción a imponer, si los operadores no cumplen con el deber legal de seguridad cibernética, con la implementación de planes de emergencia para incidentes, el abordar los riesgos oportunamente tales como virus informáticos, ataques en línea, robos o filtración de datos y cualquier forma de riesgo que ponga en riesgo la seguridad de la red. Este país por las obligaciones que deposita a los operadores de red y que establece sanciones frente a la negligencia ante estas, muestra un nivel alto y suficiente en la regulación de este indicador.

Por su parte, España contiene la regulación de las sanciones ampliamente en su Ley orgánica 3/2018 y a su vez se complementa con los medidores de la sanción con el Reglamento Europeo 679/2016. España sanciona a sus operadores de red en razón de la violación de los datos personales y establece sus mediciones considerando varios aspectos de la calidad tanto de los datos como de las personas que infringieron los mismos, lo anterior con el fin de establecer una sanción proporcionada, tales aspectos son, entre ellos la naturaleza de la infracción, la gravedad, su duración en el tiempo, el número de personas afectadas, el alcance del daño, entre otras características que permiten un estudio detallado de la conducta desviada y de la sanción como tal. También es aplicable la publicación tanto de la sanción como del infractor en el Boletín Oficial del Estado. En este orden de ideas, España se encuentra en un nivel suficiente de protección de los datos personales por lo estricto en lo que basa sus sanciones.

Por parte de Brasil, contiene en su Ley de protección de datos personales, en cual sanciona todas aquellas conductas contrarias a esta ley y que signifiquen una violación a los derechos de intimidad, privacidad, honor, imagen y la dignidad humana. Para imponer sanciones se llevará a cabo primero un procedimiento administrativo amplio para la defensa del investigado, después de agotado ésta se impondrán sanciones pecuniarias de hasta cincuenta millones reales; por consiguiente, también se aplicará como sanción la publicación de la misma y del infractor después de haberse investigado a cabalidad, la eliminación y bloqueo de los datos infringidos, suspensión o prohibición de la actividad de tratamiento. Por lo anterior, Brasil cuenta con una suficiente protección de los datos personales por el control que otorga a los mismos y la forma detallada en que basa sus sanciones.

Por parte de Colombia, ha establecido unas sanciones con multa por la violación a las redes de internet que proporcionen un daño en la misma. Se cuenta con las sanciones establecidas en la Ley Habeas Data graduando las misma valorando ciertos aspectos, entre ellos, el nivel del daño, el provecho económico obtenido, la reiteración de la conducta, entre otros, son agravantes de la multa o sanción. Sin embargo, para la atención de las vulneraciones de los datos personales y las sanciones, no se cuenta con un órgano u oficina unificado que se encargue del cumplimiento de las mismas, esto no permite contar con una total seguridad jurídica, pues en el ámbito privado para la atención a las vulneraciones y sanciones se cuenta con una oficina ubicada en la Super Intendencia de Industria y Comercio y para atender las vulneraciones en el ámbito privado se cuenta con la Procuraduría General de la Nación.

Indicador # 10. existencias de un órgano de control y vigilancia de los datos personales

Tabla 13 Medición cualitativa

Medición Cualitativa	
EE.UU	INSUFICIENTE
CHINA	SUFICIENTE
ESPAÑA	SUFICIENTE
BRASIL	SUFICIENTE
COLOMBIA	INSUFICIENTE

Con relación a los órganos de control y vigilancia de la protección de los datos personales, en los países como España, China y Brasil disponen de un órgano de vigilancia y monitoreo independiente encargado solamente de la vigilancia del cumplimiento de sus leyes nacionales sobre la protección de los datos personales en redes sociales e internet. En España como se especificó anteriormente, cuenta con La Agencia Española de Protección de Datos como órgano individual, mismo que está regulado en el artículo 44 de la Ley Orgánica 3/2018, la cual España dedica un capítulo completo a la especificación y profundización de la competencia de este órgano de control y hasta dónde llega su alcance, detallando desde las funciones y potestades hasta los cargos a desempeñar en esta organización otorgando obligaciones concretas a cada uno así como también contar con un presupuesto económico que garantice su autonomía y actividad, también este órgano lleva a cabo unos planes de auditoría preventiva que permita la adaptación de los titulares de los datos a las disposiciones legales de este país. En Brasil igualmente se cuenta con una regulación amplia al respecto que cuenta con el desglosamiento de los directivos y miembros del órgano de control, este mismo también es el encargado de imponer sanciones, implementar mecanismos de queja por el incumplimiento de la ley entre otras disposiciones. Estos dos últimos países se encuentran en un nivel alto de protección por contar con un ente de vigilancia dedicado exclusivamente a la protección de los datos personales y una regulación detallada del mismo. A diferencia de China que, si bien cuenta también con un órgano de control independiente, no hay una regulación tan minuciosa al respecto, sin embargo los entes de control de China hacen parte del departamento de información de la red nacional coadyubada con otros entes como lo son el departamento de telecomunicaciones del Consejo de Estado y el departamento de seguridad pública que se unen entre sí para el apoyo de la red cibernética, lo que comprende que en este país hay un mayor interés en el monitoreo y rastreo efectivo de posibles riesgos y vulneraciones a los datos personales.

Por parte de Estados Unidos y Colombia, ambos tienen un ente de control que no es encargado principalmente de vigilar y mitigar las posibles violaciones a los datos personales, pues como se dijo anteriormente, EEUU cuenta con la Comisión Federal de comercio que tiene como función principal el control de la competencia desleal, como de la compra y venta de los datos; por otra parte, Colombia cuenta como ente de control con la Super Intendencia de Industria y comercio que es encargada vigilar la competencia en el mercado, protección de los consumidores y datos personales. Por consiguiente, ni Estados Unidos ni Colombia cuentan con un órgano de control y

vigilancia independiente que sea dirigido únicamente a la investigación y monitoreo de la protección de los datos personales como se vio en los países como España, Brasil y China.

En este orden de ideas, España, Brasil y China tienen un buen grado de protección en relación con el órgano de control y vigilancia, siendo España y Brasil los de un nivel más alto de protección por contar con un órgano individual muy regulado y detallado en su conjunto, otorgando más seguridad jurídica por hacer cumplir sus leyes de protección de datos tan estricta y organizadamente.

Aportes a Colombia de la comparación de su legislación con la de los demás países en relación con los indicadores planteados.

La comparación aplicada permitió identificar varios aspectos importantes que contienen algunos países dentro de sus legislaciones sobre la protección de los datos personales en medios de internet que demuestra que hay formas más completas y garantistas para darle una protección a los datos personales que circulan por estos medios, cuya aplicación sería útil en orden del crecimiento de Colombia frente a esta cuarta revolución tecnológica. Estos aspectos son el contar con un órgano de vigilancia unificado de los datos personales dedicado exclusivamente en la materia que permita un mayor grado de control con la protección de los datos personales, que haga cumplir la ley y sus sanciones, otro aspecto es que exista una ley unificada e independiente para la regulación de los datos personales en el ámbito del internet, al igual que una ley única la protección de los datos personales de los menores de edad en línea, que haga efectivo esa protección especial y constitucional que la Constitución les otorga, así como controlar con mayor profundidad la obtención del consentimiento del titular de los menores para el tratamiento de los datos, entre otros aspectos como contar con más procedimientos internos de control para solicitar la trasferencia internacional de los datos y para la obtención del consentimiento en línea para el tratamiento de los datos.

Conclusiones

Con fundamento en los anteriores resultados se puede concluir que es muy importante que cada país se ajuste a una actualidad que ha traído al mundo avances tecnológicos sin precedentes. Es vital de contar con un régimen regulatorio en el ámbito de protección de los datos personales en el uso masivo de las redes sociales e internet, teniendo en cuenta todas las practicas que en las mismas se ha ido implementando en el paso de los años como usos de herramientas en el ciberespacio de recolección, uso y tratamiento de los datos y considerando que cada día hay más usuarios en estas redes.

La comparación realizada entre los países se hizo con base a los indicadores construidos para medir el nivel de protección de los datos personales en ámbito de redes sociales e internet de los países escogidos, lo anterior permitió establecer que España y China, son los países más garantistas, rigurosos y coherentes en la protección de datos personales y del ejercicio del uso y tratamiento de los mismos en las redes sociales e internet, por contar con elementos esenciales que estructuran ampliamente este régimen sin privarse ni dejar sin efectos ningún aspecto que pueda generar un riesgo o un daño a una persona natural por infringir sus datos personales y su vida privada. Los países clasificados con un mayor grado de protección cuentan con órganos de control y leyes unificadas dedicadas exclusivamente a la vigilancia y control de los datos personales en internet, así como aspectos generales como limitaciones que terminan de complementar las leyes en la seguridad del ciberespacio, entre ellas, el apoyo a instituciones de educación superior, empresas y capacitaciones para ejercer la educación, acogiendo métodos que permitan la creación de nuevos sistemas de seguridad y rastreo en el especto electromagnético. Otros aspectos generales hallados en el ejercicio de investigación son normas sobre la cuantificación económica de los datos personales recolectados y de regulaciones en torno a las bases de datos automatizadas que pueden ser objeto de estudio en futuras investigaciones. Otro aspecto interesante que se ha encontrado que podría ser objeto de futuros estudios es la protección de los datos personales abordada desde el punto de vista jurisprudencial y el desarrollo que se da a esta en la jurisprudencia.

El proyecto realizado contribuye de manera importante al estudio de la protección de los datos personales, esto al identificar puntos comunes en las legislaciones cuya presencia indica un adecuado nivel de protección, los cuales sirven para medir el nivel de protección brindado por las legislaciones.

La importancia y la necesidad que se tiene en Colombia, de contar con un régimen de protección de los datos en redes sociales e internet es cada vez más evidente. Nos encontramos en una era digital donde las relaciones y comunicaciones sociales han cambiado a ser más instantáneas e inmediatas, debido al uso continuo que hay hoy en día de distintas tecnologías como la web, aplicaciones, redes sociales, teléfonos inteligentes, búsquedas en internet, entre otros muchos que, con su crecimiento y uso continuo por parte de sus usuarios, generará cada vez más información y datos. Colombia, con respecto a otros países, cuenta con un régimen de protección de datos que, no cumple con un estándar suficiente y adecuado de protección, como lo sería el de la Comisión Europea, pues el modelo europeo es caracterizado por ser el más proteccionista y estricto en este sentido. En un país es de suma importancia establecer un régimen de protección de los datos personales en internet porque esto puede conllevar a la posibilidad de sumar a la seguridad jurídica

de la información ciudadana, aporta a la competitividad con otros países que conllevan el intercambio de información internacional porque causa seguridad al negociar y por considerarse la protección de los datos personales como esencial en una sociedad democrática.

Se logró ver que Estados Unidos al no contar con una ley de carácter nacional que regule el tema y al dejarlo principalmente en manos de la autorregulación de la industria tecnológica, fue el país que peor calificación obtuvo en la comparación del nivel de protección de los datos personales entre las legislaciones analizadas.

De igual manera se identificó con el estudio de las legislaciones de los países, que un país que cuenta con una legislación de carácter nacional y unificada en el tema, en términos generales garantiza una mejor protección a los datos personales.

Bibliografía

Alaimo, C. y Kallinikis, J. (2017). Computing the everyday: Social media as data platforms. *The Information Society*, 33 (4) 175-191. doi: 10.1080/01972243.2017.1318327

Alcaraz, M. (2014). Internet de las cosas. Universidad Católica Nuestra Señora de la Asunción, 1-27. Recuperado de: http://jeuazarru.com/wp-content/uploads/2014/10/Internet-of-Things.pdf

Antevio. (2016). Breve historia de las redes sociales. *Antevio*. Recuperado el 10 de agosto de 2020, de: https://www.antevenio.com/blog/2016/10/breve-historia-de-las-redes-sociales/

Aránguiz, M. (2020). Sobre la protección de datos personales en China. *Diario Financiero*. Recuperado el 11 de noviembre de 2020 de: https://www.df.cl/noticias/opinion/columnistas/df-conexion-a-china-sobre-la-proteccion-de-datos-personales-en-china/2020-10-26/195056.html

Arevalo, J. (2007). Gestión de la Información, gestión de contenidos y conocimiento. *II Jornada de trabajo del Grupo SIOU*, 1-15. Recuperado el 10 de agosto de 2020 de: http://eprints.rclis.org/11273/1/Jornadas_GRUPO_SIOU.pdf

Arias Orozco, E. (2010). Curso de investigación para docentes de la Catolica del Norte fundación universitaria - Tema 7. *Fundación Universitaria Católica del Norte.* Recuperado el 23 de junio de 2010 de: https://www.ucn.edu.co/Biblioteca%20Institucional%20Cemav/Curso-basico-investigacion/11Tema7.html#:~:text=Investigaci%C3%B3n%20%E2%80%93%20Acci%C3%B3n%3A%20el%20alcance%20en,permitan%20transformar%20la%20realidad%20estudiada.

Asociación por los Derechos Civiles. (2016). El sistema de protección de datos personales en América Latina: Oportunidades y desafios para los derechos humanos. *Asociación por los Derechos Civiles*. Recuperado de: https://www.internetlab.org.br/wp-content/uploads/2017/03/Sistema-proteccion-datos-personales-LatAm.pdf

Bnamericas. (2020). Nueva ley de protección de datos crea desafíos y oportunidades para Brasil. *Bnamericas*. Recuperado el 11 de noviembre de 2020 de: https://www.bnamericas.com/es/reportajes/nueva-ley-de-proteccion-de-datos-crea-desafios-y-oportunidades-para-brasil

Bru, E. (2007) La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *Revista de Internet, Derecho y Política.* Recuperado de: https://www.redalyc.org/pdf/788/78812861008.pdf

Cadwalladr, C. y Graham-harrison, E. (17 de Marzo de 2018). Revelead: 50 million Facebook profiles harvested for Cambridge Analytica in major dara breach. The Guardian. Retrieved from: http://freestudio21.com/wp-content/uploads/2018/04/50-million-fb-profiles-harvested-by-cambridge-analitica.pdf

Castillo, C. (2000) Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información*. Revista Derecho y conocimiento, vol. 1, pags. 35-48, ISSN 1578-8202.* Recuperado de: https://core.ac.uk/download/pdf/60634513.pdf

California Consumer Privacy Act. California, Estados Unidos. (23 septiembre de 2018). Recuperado de: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

Carreño, I. (21 de febrero de 2020). Ley de Protección de Datos en Brasil entró en vigor pero no en su totalidad. *Digital Policy Law*. Recuperado el 3 de agosto de 2020 de: https://digitalpolicylaw.com/ley-de-proteccion-de-datos-en-brasil-entro-en-vigor-pero-no-en-su-totalidad/

Castellano, S. (2015). El reconocimiento del derecho al olvido digital en España y la UE: efectos tras la sentencia del TJUE de mayo de 2014, Barcerlona, España: *Editorial Bosch.* Recuperado de: http://www.wke.es/MK/PDF/El-reconocimiento-del-derecho-al-olvido-digital-en-Espana-y-en-la-UE/files/assets/common/downloads/publication.pdf

Celaya, J. (2008). La empresa en la web 2.0. Barcelona, España: *Gestion 2000*.

Children´s Online Privacy Protection Act. Federal Trade Comision, California, Estados Unidos, 21 de octubre de 1998. Recuperado el 21 de junio de 2020 de: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Civil Code of the State of California. California Legislative Information California, Estados Unidos, 1872. Recuperado el 2 de agosto de 2020 de: https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=CIV

Colombia Legal Corporation. (2019). ¿Conoces el Derecho de Habeas Data en Colombia?. *Colombia Legal Corporation*. Recuperado el 2 de Agosto de 2020 de: https://www.colombialegalcorp.com/blog/derecho-de-habeas-data/#:~:text=El%20Derecho%20de%20Habeas%20Data%20consiste%20en%20Colombia%20por%20permitir,bases%20de%20datos%20del%20pa%C3%ADs.&text=En%20esta%20ley%20est%C3%A1%20contemplado,la%20informaci%C3%B3n

Comisión Europea. (s.f.). ¿Qué son los datos personales?. *Web oficial de la Unión Europea*. Recuperado el 12 de Agosto de 2020 de: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es#referencias

Comisión Europea. (s.f.). What constitutes data processing?. *Web oficial de la Unión Europea*. Recuperado el 10 de agosto de 2020, de https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_es

Coneval. (2013). Manual para el diseño y construcción de indicadores: Instrumentos principales para el monitoreo de programas sociales en México. *Consejo Nacional de Evaluación de la Política de Desarrollo Social*. Recuperado el 10 de noviembre de 2020 de: https://www.coneval.org.mx/Informes/Coordinacion/Publicaciones%20oficiales/MANUAL_PARA_EL_DISENO_Y_CONTRUCCION_DE_INDICADORES.pdf

Constitución española. (1978). España. Recuperado el 1 de junio de 2020 de: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf

Constitución Política Colombiana. (1991). Colombia. Recuperado el 3 de junio de 2020 de: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Constitución Política de la República Federativa del Brasil. (1988). Brasil. Recuperado el 1 de junio de 2020 de: https://pdba.georgetown.edu/Constitutions/Brazil/esp88.html

Cybersecurity Law of the People's Republic of China. [Ley de ciberseguridad de la República Popular China] (1 de junio de 2017). China. Recuperado el 12 de junio de 2020. Recuperado de: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

Dane. (s.f.). Guía para el diseño, construcción e interpretación de indicadores. *Departamento Administrativo Nacional de Estadísticas*. Recuperado el 20 de noviembre de 2020, de https://www.dane.gov.co/files/planificacion/fortalecimiento/cuadernillo/Guia_construccion_interpretacion_indicadores.pdf

Davara, I. (2017). Regulación en internet y políticas públicas para su despliegue: Modelos de privacidad y protección de datos personales. *Slideshare*. Recuperado el 10 de noviembre de 2020 de: https://www.slideshare.net/FranciscoJavierCervi2/modelos-de-privacidad-y-proteccin-de-datos-francisco-javier-cervigon-ruckauer

De salas Nestares, M. (2012). La publicidad en las redes sociales. De lo intrusivoa a los consentido. *ICONO14 Revista Científica De Comunicación Y Tecnologías Emergentes*, 75-84. doi:https://doi.org/10.7195/ri14.v8i1.281

Debitoor. (s.f.). Glosario de contabilidad Derecho al olvido. *Debitoor*. Recuperado el 11 de noviembre de 2020 de: https://debitoor.es/glosario/derecho-al-olvido

Decreto 1377. (2013). Colombia. Recuperado el 12 de mayo de 2020 de: http://www.suin-juriscol.gov.co/viewDocument.asp?id=1276081

E-Health Reporter. (2020). Leyes de protección de datos durante la pandemia de COVID-19. *E-Health Reporter*. Recuperado el 10 de mayo de 2020 de: https://ehealthreporter.com/es/noticia/leyes-de-proteccion-de-datos-durante-la-pandemia-de-covid-19/

El Tiempo. (20 de Mayo de 2020). A juicio disciplinario dos generales (r) por perfilamientos ilegales. *El Tiempo*. Recuperado de: https://www.eltiempo.com/justicia/investigacion/procuraduria-cito-a-juicio-a-13-militares-por-perfilamientos-ilegales-497586

Feng, J., De Andrade, L. y Torres, V. (2010). Estados Unidos Patente nº US9262517B2. Recuperado el 10 de mayo de 2020 de: https://patents.google.com/patent/US9262517B2/en

Fernández, A. L. y de Lama, S. (2018). La cuarta revolucipon industrial y la agenda digital de las organizaciones. *Economía industrial*, 95-104. Recuperado el 12 de junio de 2020 de: https://dialnet.unirioja.es/servlet/articulo?codigo=6535711

Frassia, Mercedes. (s.f.). Introducción a las bases de datos, un poco de teoría. Recuperado el 20 de julio de 2020 de: https://pdf4pro.com/cdn/introducci-211-n-a-las-bases-de-datos-un-poco-de-teor-237-a-55e1c2.pdf

Gasca-hurtado, G.P. y Machuca-villefas,L. (2019). Era de la cuarta revolución industrial. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 11-15. doi:http://dx.doi.org/10.17013/risti.34.0

Gil, E. (2016). Big data, privacidad y protección de datos. *Agencia Española de Protección de datos personales*. Recuperado de: https://d1wqtxts1xzle7.cloudfront.net/59120887/big-data_privacidad_protecion_de_datos_libro20190503-117965-f78lez.pdf?1556904273=&response-content-disposition=inline%3B+filename%3DBig_data_privacidad_y_proteccion_de_dato.pdf&Expires=1600215295&Signature=b

Gonzalez, F. (2019). Big data, algoritmos y política: las ciencias sociales en la era de las redes digitales. *Universidad Central de Chile,* Santiago, Chile, 267-280. Recuperado de: https://scielo.conicyt.cl/pdf/cmoebio/n65/0717-554X-cmoebio-65-00267.pdf

Gordillo Triana, J y Restrepo Yepes, O. (2004). Introducción al análisis del derecho. *Universidad del Rosario. Estud. Socio-Juríd*., Bogotá (Colombia). Recuperado de: http://www.scielo.org.co/pdf/esju/v6n2/v6n2a12.pdf

Gurtubay, M. (1994) Análisis comparado de las Legislaciones sobre Protección de Datos de los Estados Miembros de la Comunidad Europea. *Derecho Público y Ciencias Histórico-Jurídicas. P.397-420.* Recuperado de: https://dialnet.unirioja.es/descarga/articulo/248383.pdf.

Hellasconsultores. (2013). Tratamiento de datos personales, privacidad y redes sociales. Recuperado el 15 de Junio de 2020. Recuperado de: https://www.helasconsultores.com/hemeroteca/2013/TRATAMIENTO-DATOS-PERSONALES-PRIVACIDAD-REDES-SOCIALES-12684.html#

Huerta Anguiano, J. A. (2020). "Naturaleza intrínseca", "contexto" o "finalidad" en la determinación del carácter sensible de los datos personales. *Estudios en derecho a la información*, 1-31. doi:http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

Iguarán Osorio; y Muñoz Jiménez. (2012). Habeas data: desarrollo normativo y jurisprudencial en Colombia. *Universidad EAFIT,* 1-57. Colombia. Recuperado de: https://repository.eafit.edu.co/bitstream/handle/10784/12075/Miguel%C3%81ngel_IguaranOsorio_Rafael_Mu%C3%B1ozJim%C3%A9nez_2012.pdf?sequence=2

INTECO, Instituto Nacional de Tecnologías de la Comunicación y AEPD, Agencia Española de Protección de Datos. (2009). Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online. Recuperado de: https://www.uv.es/limprot/boletin9/inteco.pdf

International Institute for Management Development. (2020). The IMD World Digital Competitiveness Ranking 2020 results. IMD. Recuperado el 20 de noviembre de 2020. Recuperado de: https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2020/

Joyanes Aguilar, L. (2013). Big Data, Análisis de grandes volúmenes de datos en organizaciones. Mexico: *Alfaomega Grupo Editorial*. Recuperado de: https://books.google.es/books?hl=es&lr=&id=1GywDAAAQBAJ&oi=fnd&pg=PT6&dq=Joyanes,+L,+2013&ots=_XN4N74eZO&sig=eQTgcqCrfj7aFd60ipKynwGfyxM#v=onepage&q&f=false

Ley estatutaria 1581, Habeas Data. Colombia. 17 de octubre de 2012. Recuperado el 12 de junio de 2020. Recuperado de: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

Ley n. 13.709 / 2018 - Prevé la protección de datos personales y cambios (Derechos civiles brasileños Marco para Internet). Brasil. Recuperado el 14 de junio de 2020. Recuperado de: https://www.lgpdbrasil.com.br/wp-content/uploads/2019/06/LGPD-english-version.pdf

Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. España. 5 de diciembre de 2018. Recuperado el 13 de junio de 2020. Recuperado de: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Licklider, J. (2002). Historia de Internet. 1-14. Recuperado de: https://cmapspublic2.ihmc.us/rid=1239136955718_1163871558_10281/historia%20internet.pdf

March, A. (octubre, 2012). La digitalización de la comunicación humana: alteraciones y cambios en la percepción. *Creación y Producción en Diseño y Comunicaión (Universidad de Palermo),* 16-19. Recuperado de: http://fido.palermo.edu/servicios_dyc/publicacionesdc/archivos/416_libro.pdf#page=16

Marqués, A. (2011). Bases de datos. *Universitat Jaume I*. Recuperado de: http://repositori.uji.es/xmlui/handle/10234/24183

Martínez Devia, A. (2019). La inteligencia artificial, el big data y la era digital ¿una amenaza para los datos personales? *Rev. Prop. Inmaterial*, 1-19. Universidad de los Andes, Chile. Recuperado de: https://poseidon01.ssrn.com/delivery.php?ID=549006098115007002114085114120104064018071056080004037007125090119094127077085117004037020023014049096033102027094126011025100020055059047019086091108089086011018064048036095029011097085096031020019091126127072 1

Martínez, N. (Junio, 2019). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *AIS: Ars Iuris Salmanticensis*, 7, 254-259. Ediciones Universidad de Salamanca. España. Recuperado de: https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Ley+Org%C3%A1nica+3%2F2018%2C+de+5+de+diciembre%2C+de+Protecci%C3%B3n+de+Datos+Personales+y+garant%C3%ADa+de+los+derechos+digitales.&btnG=

Mayer, V. y Cukier, K. (2013). Big Data: La revolución de los datos masivos. Madrid: *Turner Publicaciones*. Recuperado de: https://books.google.es/books?hl=es&lr=&id=uO9FbEcaMpkC&oi=fnd&pg=PA11&dq=Mayer,+V.+y+Cukier,+K.,+2013&ots=V_xS1frICV&sig=O2uf_V8WPW6PtINszXsSf7TdUY0#v=onepage&q=Mayer%2C%20V.%20y%20Cukier%2C%20K.%2C%202013&f=false

Medina, J; López, L y Díaz, A. (2012). La medición de datos cualitativos, una tendencia en investigación social: análisis del caso de la facultad de contaduría y administración, unidad Culiacán. *Facultad de Contaduría y Administración, Unidad Culiacán*, 8(2). Recuperado de: http://uaim.edu.mx/webraximhai/Ej-24articulosPDF/ARTICULO_07.pdf

Molins Renter, A. (5 de Enero de 2020). *La Vanguardia*. Recuperado de: https://www.lavanguardia.com/vida/20200105/472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio-electronico.html

Morales, F. (2012). Conozca 3 tipos de investigación: Descriptiva, Exploratoria y Explicativa. 11. Recuperado el 10 de junio de 2020. Recuperado de: http://www.creadess.org/index.php/informate/de-interes/temas-de-interes/17300-conozca-3-tipos-de-investigacion-descriptiva-exploratoria-y-explicativa

OEA, Organización de los Estados Americanos. (3 de abril de 2012). Estudio comparativo: Protección de datos en las américas. *Organización de los Estados Americanos, Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos*. Recuperado de: https://www.oas.org/es/sla/ddi/docs/CP-CAJP-3063-12.pdf

Oliván, R. (2016). La Cuarta Revolución Industrial, un relato desde el materialismo cultural. *Revista de Estudios Urbanos y Ciencias Sociales*. Volumen 6, número 2, páginas 101-111. Recuperado de: http://repositorio.ual.es/bitstream/handle/10835/4809/LA%20CUARTA%20REVOLUCION%20INDUSTRIAL.pdf

Pérez, M. (28 de mayo de 2020). *Digital Policy Law*. Recuperado el 3 de agosto de 2020. Recuperado de: https://digitalpolicylaw.com/china-avanza-en-el-marco-regulatorio-de-la-privacidad-individual/

Redacción BBC News Mundo. (24 de Julio de 2019). BBC News Mundo. Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios. Recuperado de: https://www.bbc.com/mundo/noticias-49093124

Reglamento sobre la protección de la información personal de los niños en línea. (1 de octubre 2019). China. Recuperado el 13 de junio de 2020, de Reglamento sobre la protección de la información personal de los niños en línea. Recuperado de: https://perma.cc/2RJZ-XN98

Remolina, N. (2010) ¿tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *Revista Colombiana de Derecho Internacional*, 489-524. Recuperado de: https://revistas.javeriana.edu.co/index.php/internationallaw/article/view/13847/11142

Rodríguez Zubieta, E. y Cordero Saavedra, A. (2018). Ciberseguridad: los acuerdos de cooperación para el tratamiento de las amenazas en el ciberespacio. El caso de Estados Unidos y China. *Universidad de la Salle*. facultad de ciencias económicas y sociales. Colombia. Recuperado de: https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1083&context=negocios_relaciones

Roig, A. (2009). E-privacidad y redes sociales. *Revista de internet, derecho y política* (9), 42-52. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=3101802

Romero, P. (19 de diciembre de 2013). Protección de Datos multa a Google por 'vulnerar gravemente' los derechos de los ciudadanos. *El Mundo*. Recuperado de: https://www.elmundo.es/tecnologia/2013/12/19/52b2dbd322601d6c608b456c.html

Ros, M. (2009). Evolución de los servicios de redes sociales en internet. *El profesional de la información*, 552-557. Recuperado de: https://core.ac.uk/download/pdf/204293563.pdf

Rosenberg, M. Confessore, N. y Cadwalladr, C. (18 de Marzo de 2018). How Trump Consultants Exploited the Facebook Data of Millions [La empresa que explotó millones de datos de usuarios de Facebook] *The New York Times*. Recuperado de: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Ruiz, C. y Pérez, G. (2016) El uso de las nuevas tecnologías y los derechos humanos. *Revista Dfensor.* Recuperado de: https://cdhcm.org.mx/wp-content/uploads/2016/09/dfensor_06_2016.pdf

Sánchez Pérez, G y Rojas González, I. (7 de junio de 2012). Leyes de protección de datos en el mundo y la protección de datos biométricos. Parte I. *Revista .Seguridad*. Recuperado de: https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

Sánchez, L. J. (7 de Diciembre de 2018). Hoy viernes entra en vigor la nueva LOPDGDD y sus nuevos 17 derechos digitales que entroncan con el RGPD. *Confilegal*. Recuperado de: https://confilegal.com/20181207-hoy-viernes-entra-en-vigor-la-nueva-lopdgdd-y-sus-nuevos-diecisiete-derechos-digitales-que-entronca-con-el-rgpd/

Schuschny, S. y Soto, H. (mayo de 2009). Guía metodológica: Diseños de indicadores compuestos de desarrollo sostenible. *Cepal*. Comisión Económica para América Latina y

el Caribe. Recuperado de: https://repositorio.cepal.org/bitstream/handle/11362/3661/S2009230_es.pdf?sequence=1&isAllowed=y

Stranieri, S. (17 de septiembre de 2019). *Ipswitch*. Leyes Globales De Privacidad De Datos: USA, UE, China Y Más. Recuperado de: https://blog.ipswitch.com/es/leyes-globales-de-privacidad-de-datos-usa-ue-china-y-m%C3%A1s

Trujillo, C. (2017). Aproximación a la regulación del consentimiento en el reglamento general de protección de datos. *Universidad de La Laguna. Facultad de Derecho*. España. Recuperado de: https://riull.ull.es/xmlui/handle/915/7948

Van Dijck, J. (2016). La cultura de la conectividad: una historia crítica de las redes sociales. *Siglo XXI Editores*. Argentina. Recuperado de: http://catedradatos.com.ar/media/La-cultura-de-la-conectividad_-Jose-Van-Dijck.pdf

Vázquez, S. (30 de junio de 2015). Tecnologías de almacenamiento de información en el ambiente digital. e-ciencias de la información - *Universidad de Costa Rica*, 5(2). Recuperado el 2020 de 15 de agosto. Recuperado de: https://revistas.ucr.ac.cr/index.php/eciencias/article/view/19762

Villalba, C. (1993). Redes sociales: un concepto con importantes implicaciones en la intervención comunitaria. Madrid, España: *Colegio Oficial de Psicólogos de Madrid*. Recuperado de: http://www.copmadrid.org/webcopm/publicaciones/social/1993/vol1/arti6.htm