MARIA PAULA ÁLVAREZ ARIAS

ANÁLISIS DE REGÍMENES DE PROTECCIÓN DE DATOS PERSONALES, CASOS EUROPEO, ESTADOUNIDENSE Y COLOMBIANO

(Maestría en Derecho Económico con énfasis en Derecho Económico Internacional, Comercio, Transacciones e Inversión)

Bogotá D.C., Colombia

2019

UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

MAESTRÍA EN DERECHO ECONÓMICO CON ÉNFASIS EN DERECHO ECONÓMICO INTERNACIONAL, COMERCIO, TRANSACCIONES E INVERSIÓN

Rector:	**Dr. Juan Carlos Henao Pérez**
Secretaria General:	**Dra. Martha Hinestrosa Rey**
Decana Facultad de Derecho:	**Dra. Adriana Zapata Giraldo**
Director (E) Departamento Derecho Económico:	**Dr. José Manuel Álvarez Zarate**
Director:	**Dr. Julián Zuluaga Torres**

TABLA DE CONTENIDO

Pág.

ÁREA TEMÁTICA

Regímenes de protección de datos personales en los casos Europeo, Estadounidense y Colombiano. Inteligencia artificial y la protección de los datos personales.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) 2016/679, Decisión 2000/520 de la comisión de las comunidades europeas, marco para los flujos transatlánticos de datos: el Escudo de la privacidad UE – EE.UU o “privacy shield”, la Convención 108 (pautas sobre Inteligencia Artificial y Protección de Datos) del Comité Consultivo de la Convención para la Protección de las Personas frente al manejo de los datos personales; la Ley 1581 de 2012 y Decretos reglamentarios.

PROBLEMA

¿Cuáles son los desafíos en materia de la normatividad de protección de datos para Colombia con el desarrollo las nuevas tecnologías de la cuarta revolución industrial, en particular la Inteligencia artificial/ machine learning y el internet de las cosas?

HIPÓTESIS

Considerando el creciente flujo transfronterizo de los datos personales, además de la implementación de herramientas relacionadas con las nuevas tecnologías, cada vez es más riesgoso el ejercicio de los derechos de los titulares de este tipo de información, pues en pocas oportunidades es clara la finalidad de la recolección de los datos y su destino.

Adicionalmente, en el ejercicio diario por medio de varias formas como cookies, el acceso a ubicación geográfica, la creación de un usuario u otorgar los datos personales se les impone a los consumidores otorgar sus datos para poder acceder a contenidos y servicios por medio de páginas web o aplicaciones, sin tener la posibilidad de no entregarlos y de la misma forma acceder a las ofertas de empresarios alrededor del mundo.

Las herramientas que se deben utilizar con miras a resolver los problemas de protección de datos personales no deben limitarse a emitir nuevas leyes en países con relevancia en flujos transfronterizos de información, sino que también debe realizarse una campaña de concientización a los consumidores que aceptan las políticas de privacidad y tratamiento de datos, pues son pocos los usuarios que efectivamente se dedican a leer las políticas y son menos los que realmente conocen las implicaciones de acceder a las condiciones de las grandes empresas. Igualmente, deben materializarse los derechos de los consumidores, al otorgar la opción de rechazar las imposiciones dadas por las compañías tecnológicas y poder efectivamente ingresar a la información dispuesta por los empresarios tecnológicos.

Es decir que debe buscarse el balance entre el desarrollo de los negocios y la protección de la privacidad, no por medio de la implantación de un nuevo

modelo, sino de agregar enmiendas a las obligaciones de los responsables en el manejo de datos en el sentido de no limitar el ejercicio de los consumidores mundiales y a nivel transnacional, respetando de la misma manera los derechos fundamentales a la privacidad y datos personales frente a la libertad económica de los encargados de realizar operaciones con la información personal. La implementación de recursos similares al “privacy shield” o autocerficiación de mínimos de protección son una opción que puede conducir a generar equilibrios entre el comercio y la protección de los datos personales.

OBJETIVOS

- **Principal:**

Evaluar el ejercicio de la protección del derecho fundamental del manejo de los datos personales de los usuarios tanto a nivel mundial y colombiano, considerar softwares que manejan algoritmos de inteligencia artificial e internet de las cosas.

- **Específicos:**

    - Estudiar el régimen de amparo del régimen europeo sobre la protección de datos personales.

    - Ahondar en el cuidado de los datos personales en Estados Unidos de América.

    - Revisar los argumentos a favor y en contra de la regulación colombiana sobre la protección de la información.

    - Recomendar si Colombia debe o no reforzar los criterios de protección en el uso de las tecnologías de comunicación e información en desarrollo.

INTRODUCCIÓN

En los días que transcurrimos la mitad de la población está conectada por medio del internet, con cifras cercanas al 89% de norteamericanos y 70% de europeos. (Gravrock, 2019) Atravesamos por un proceso que los economistas han denominado la cuarta revolución industrial, un fenómeno que estará marcado por la transformación en aspectos tecnológicos, sociales, económicos y que resultará en la mejora y automatización de los medios de producción por medio de la instauración de tecnologías digitales y ciberfísicas. De tal forma que en el futuro cercano veremos la incursión de fábricas verdaderamente inteligentes con herramientas como son el internet de las cosas, computación en la nube, big data, inteligencia artificial y Blockchain, entre otros.

En el transcurso de cada revolución, determinada materia prima tuvo particular relevancia, pues recursos como fueron el carbón, el acero, el petróleo y la electricidad marcaron la diferencia en cada transformación. El recurso clave a explotar en la revolución que transitamos son los datos, de tal forma que se ha afirmado varias veces que ahora valen más que el petróleo, considerando que es a través del uso de los datos que se implementan la innovación y las tecnologías.

De ahí, que las empresas tecnológicas sean las empresas más valiosas a nivel mundial, pues que las compañías que para el 2018 fueron las más valiosas en el mercado de tecnología[1], hayan cimentado su negocio en la numerosa cantidad de datos de usuarios de forma electrónica, y el tratamiento integrado

[1] Como Amazon con un valor de $802, 18 mil millones de dólares; Microsoft que ascendió a un valor de $ 789,25 mil millones de dólares; Alphabet (empresa matriz de Google) cuyo valor fue de $737,37 mil millones de dólares; Apple ascendió a $720,12 mil millones de dólares y Facebook que sumó $413,25 mil millones de dólares (FXSSI, 2019)

con tecnologías requeridas como son algoritmos, mecanismos de análisis de datos y sistemas de seguridad, es un claro ejemplo de la alta relevancia del tratamiento de datos. (Cuesta, 2019).

En efecto, las empresas a nivel mundial utilizan los datos personales para procesos de negocio y análisis de datos, con miras a determinar hábitos de consumo, comportamientos, gustos y preferencias con base en búsquedas en la web y los usos de las redes sociales. Es decir, que los datos personales son procesados por las compañías para generar conocimiento y soporte para determinar decisiones, estrategias, mercadeo y publicidad. (Barquin, 2019).

De manera que en una sociedad donde los datos tienen un papel determinante como moneda de cambio[2], se abre lugar a la paradoja entre los estándares de protección que debe tener la información personal de los consumidores de medios digitales y la promoción del comercio por medio de la utilización de las tecnologías nacientes. Como consecuencia del desarrollo de empresas que utilizan datos personales, es que los regímenes de protección cada vez más son temas controversiales y relevantes.

En vista de lo anterior, Europa es el continente más garantista de los datos personales en el mundo, pues ha dotado a los usuarios de herramientas (como el Reglamento General de Datos Personales RGDP) para que puedan saber quién tiene sus datos, y cuáles son las finalidades de la recolección, entre otros derechos. Por el contrario, en Estados Unidos este tema no ha tenido regulación a nivel federal, por ahora California ha sido el único estado en emitir una ley relacionada con la protección de los datos en el internet de las cosas, pero considerando que están en el ojo del huracán por los problemas de

[2] Los nuevos modelos de negocio desde hace un tiempo se fundamentan en un intercambio gratuito de contenidos y servicios por medio de internet a usuarios a cambio de obtener datos personales que cada vez más son tratados con intenciones de explotación económica. (Jiménez Pacheco & Leal Coronado, 2017)

seguridad y filtración de datos personales sobre todo de Facebook, cada vez más estados empiezan a regular este tema.

Por su parte, en Colombia hay leyes que regulan la protección de los datos personales con enfoque europeo, en cabeza de la Superintendencia de Industria y Comercio, entidad que ha sancionado a Facebook por incumplir deberes de seguridad.

En vista del crecimiento del uso de herramientas electrónicas para llevar a cabo transacciones entre países del mundo y el creciente flujo transfronterizo de datos como fundamento de la economía digital entre responsables de variedad de Estados, además de la implementación de nuevas tecnologías para llevar a cabo el tratamiento de los datos de usuarios en masa, como son el big data, el internet de las cosas y el learning machine o inteligencia artificial, debe observarse con lupa el cumplimiento de las disposiciones de protección de los datos personales sobre todo a nivel internacional, pues se ha evidenciado con anterioridad que hay filtración masiva de datos personales. Debe buscarse un equilibrio entre la protección de datos personales y el ejercicio del comercio, establecer si es necesario intervenir por medio de regulación o por el contrario si con las herramientas existentes es suficiente.

METODOLOGÍA

Se plantea un método cualitativo, donde se describan las disposiciones de la Unión Europea, Estados Unidos y Colombia sobre el manejo de los datos personales. Asimismo, con fundamento en fuentes documentales publicadas en la página web de firmas de abogados, la Superintendencia de Industria y Comercio, Comisión Europea, el foro económico mundial, además de artículos de periódicos como el New Yorker y Forbes entre otros y artículos de firmas de abogados publicados en línea y trabajos investigativos.

I. LA UNIÓN EUROPEA

A pesar de ser un asunto que ha tomado relevancia a través de por lo menos los últimos 50 años, es solo desde el comienzo de los años 80s que organizaciones internacionales llevaron a cabo esfuerzos considerables para establecer criterios claros sobre la protección de los datos personales. Es así como la Organización para la Cooperación y el Desarrollo Económicos (OCDE)[3], emitió en 1980 unas Directrices no vinculantes sobre protección de la privacidad y flujos transfronterizos de datos personales. Desde estas directrices se definieron los datos personales como todo tipo de información que tenga que ver con un sujeto de los datos (OCDE, 2002). En diciembre de 1990 la Asamblea General de las Naciones Unidas aprobó la Resolución 45/95, que enlista Principios rectores para la reglamentación de los ficheros computadorizados de datos personales. (Naciones Unidas, 1990).

No obstante, desde muy temprano se empezó a evidenciar que la Unión Europea pretendía establecer un régimen estricto de protección a los derechos derivados de los datos personales, pues considerando que en los países miembros de la Unión había diversidad de reglas sobre los datos personales y esto generaba obstáculos para el flujo de datos entre los países, el Consejo de Europa emitió el 28 de enero de 1981 el Convenio 108 "*para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal*" (Consejo de Europa, 1981), ratificado por 46 países. Por medio del cual se pretendió proteger el derecho fundamental de las personas a su vida privada en el ámbito automatizado ya sean de entidades públicas o privadas y

[3] organismo que pretende promover lineamientos que (…) "*mejoren el bienestar económico y social de las personas alrededor del mundo [ofreciendo] un foro donde los gobiernos puedan trabajar conjuntamente para compartir experiencias y buscar soluciones a los problemas comunes"* (OCDE, 2018)

determinar principios básicos para la protección de información personal como finalidad legítima, exactitud y obtención leal y legítima.

En desarrollo de lo anterior, el 24 de octubre de 1995 el Parlamento Europeo y el Consejo emitieron la Directiva 95/46/CE "*Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre circulación de estos datos*" (Parlamento Europeo y El Consejo de la Unión Europea, 1995).

A través de este instrumento vigente hasta mayo de 2018, determinaron el marco jurídico de la protección de datos desde un punto de vista de derecho a la intimidad. Como bien lo indica el actual Superintendente Delegado para la Protección de Datos de la Superintendencia de Industria y Comercio, este tipo de directivas, "*son el fruto de la labor de armonización de los aspectos centrales del tratamiento de datos personales. En estos se procura asegurar unos mínimos en las actividades que impliquen la recolección, almacenamiento y uso de dicha información, estableciendo unos principios sobre la materia e imponiendo, en ciertos casos, criterios de comportamiento razonable."* (Remolina Angarita, Tenorio Adame, & Quintero Navas, 2018).

Ahora bien, el 27 de abril de 2016 el Parlamento Europeo y el consejo de la Unión Europea emitieron el Reglamento (UE) 2016/679, que entró en vigencia el 5 de mayo de 2018 y derogó la anterior Directiva 95/46/CE. Considerando que la anterior directiva no fue implementada por todos los países europeos, uno de los objetivos principales de este reglamento consistió en la implantación y unificación de disposiciones de protección a los datos personales de manera uniforme en el territorio continental, es decir que es directo y por lo tanto obligatorio para todos los países que hagan parte de la Unión, sin la necesidad de incorporar formalmente las disposiciones al ámbito nacional.

Como aspecto preliminar, el consejo y el parlamento expusieron como fundamentos y motivación del vigente RGDP circunstancias como las establecidas en los considerandos 5 y 6 (Parlamento Europeo y del Consejo, 2016, pág. 2): como resultado de los avances de la tecnología y la globalización en ejercicio de la integración social y económica, se ha generado un incremento significativo de circulación de información personal entre países. Para lograr un flujo equilibrado en el mercado, se requiere la cooperación entre países con la finalidad de proteger los derechos de los usuarios y que impida la obstaculización de tales flujos de información. Además de tener en cuenta la creciente utilización de herramientas digitales por medio de las cuales sin importar el territorio se lleva a cabo el flujo de datos personales relacionados con el continente europeo.

En desarrollo de lo anterior, en el Reglamento General de Protección de Datos (RGPD), se plantea en el artículo 3 (pág. 32) la aplicación territorial de la protección, según la cual los datos se protegerán sin importar que el tratamiento se lleve a cabo en el territorio de la Unión Europea cuando se de en desarrollo de actividades de responsables dentro del territorio. También se aplica cuando el responsable del manejo no resida en el continente europeo, pero maneje datos de usuarios europeos cuando se ofrezcan bienes o servicios. En el artículo 5 (pág. 35) se plantean principios básicos que irradian las operaciones que involucran datos, como son transparencia, lealtad y licitud; una novedad frente al anterior reglamento, consistente en que la información personal debe ser recolectada con fines determinados, explícitos y legítimos y debe siempre llevar estos fines; como consecuencia de lo anterior los datos deben ser limitados a los fines señalados.

Desarrollando los principios, en el artículo 6 (pág. 36) se establece las condiciones para que el tratamiento de los datos sea legítimo, para lo cual debe presentarse consentimiento libre del usuario; se debe llevar a cabo en el

marco de operaciones en ejecución de un contrato; como requisito para cumplimiento de una obligación legal o necesaria para salvaguardar intereses de una persona; para mantener el interés público o satisfacer intereses legítimos. Asimismo, establece claras condiciones para determinar si el tratamiento de datos personales es lícito cuando la finalidad de las operaciones no fue consentida.

Posteriormente, en el capítulo 3 menciona un ramillete de derechos en cabeza de los interesados o usuarios, dentro de los cuales encontramos en su artículo 12 (pág. 39 y 40) la transparencia de la información suministrada al interesado. Tal transparencia versa sobre la identificación responsable o delegado si aplica, las finalidades de las operaciones sobre los datos y la notificación de cambio de finalidad, los destinatarios de los datos, intención de hacer transferencias a otros países, plazo de vigencia de los datos, derechos a acceso, rectificación, limitación u oposición a las operaciones con la información suministrada además de la posibilidad de reclamar ante autoridades pertinentes, si se necesita informar sobre los datos personales para ejecutar un contrato o si se utilizaría automatización de datos (Art. 13, pág. 40 y 41).

En concordancia con el principio de transparencia, se plasma en el artículo 15 (pág. 43) el derecho al acceso de información al usuario de los datos sobre todas las circunstancias que envuelvan las operaciones en donde estén incursos sus datos personales, tales como fines, destinatarios, plazo de conservación. Adicionalmente, en los artículos 16 al 21 (págs. 43 - 45) se establecen los derechos de rectificación, supresión o derecho al olvido cuando se den determinados supuestos (no son necesarios los datos respecto de los fines planteados, no hay consentimiento, tratamiento ilícito de la información, oposición), limitación, notificación, portabilidad a otro responsable y a la oposición. Los derechos como son la oposición, derecho al olvido y la

portabilidad son novedades muy relevantes que se incluyeron en el RGPD con miras a otorgarle más herramientas a los titulares de los datos personales para salvaguardar el uso que los responsables brindan a sus datos.

Más aún, en el artículo 23 (pág. 46 y 47) se establece la posibilidad que los estados establezcan limitaciones a los derechos y obligaciones de los responsables o titulares de los datos en aras de velar por la seguridad del estado, la defensa, la seguridad pública, las infracciones penales, el interés económico, la sanidad pública y la seguridad social y judicial, entre otros.

A continuación, el consejo y el parlamento describieron uno de los fundamentos más relevantes que se viene definiendo desde 1980 por la OCDE, denominado "accountability" en inglés, que traduce responsabilidad o rendición de cuentas. Tal principio fue determinado por las directrices de la OCDE sobre privacidad y flujo transfronterizo de datos personales y delimitado y ampliado en su actualización de 2013. La OCDE se limitó a definir este principio en 1980, determinando que el responsable de la información debía cumplir con todos los principios mencionados en tales directrices.

Actualmente, de acuerdo con el actual superintendente delegado para la protección de datos, "*Dicho principio exige que los responsables y encargados del tratamiento de datos, implementen medidas apropiadas, efectivas y verificables que les permitan probar el correcto cumplimiento de las normas sobre tratamiento de datos personales (…) el reto de las organizaciones frente al principio de responsabilidad va mucho más allá de la expedición de documentos, porque exige que se demuestre el cumplimiento real y efectivo cuando realizan sus funciones*" (Remolina Angarita & Alvarez Zuluaga, 2018, pág. 29).

En concordancia con lo anterior, se evidencia que en la disposición del reglamento del 16 en su artículo 24, a diferencia de las disposiciones de 1980, la responsabilidad debe ser demostrada por medio de la implantación de medidas que pueden ser técnicas y organizacionales ajustadas al caso concreto de acuerdo con riesgo inherente de los datos procesados. Teniendo en cuenta que en la parte inicial del reglamento, en los principios de manejo de datos personales se estableció en el artículo 5 numeral 2 que "*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)*" (Parlamento Europeo y del Consejo, 2016, pág. 36), queda plenamente estipulado el principio de responsabilidad demostrada en el manejo de la información personal en la directiva europea vigente.

Posteriormente se planteó una institución que tiene un tinte preventivo, se denomina "Protección de datos desde el diseño y por defecto" artículo 25 (pág. 48), según la cual el responsable de las operaciones con los datos debe tener en cuenta incluso desde antes de establecer cuales métodos utilizará para cumplir con los principios de protección de datos, como por ejemplo la minimización de datos y la seudonimización. En el artículo 35 se plasmó otra institución preventiva, denominada "Evaluación de impacto relativa a la protección de datos", en donde se estableció que, si un tratamiento involucra nuevas tecnologías y un riesgo alto de vulneración de derechos, el responsable deberá llevar a cabo un examen de impacto del tratamiento de la información.

A continuación, quedó plasmado el deber de seguridad en el artículo 32. En efecto, el responsable del manejo de los datos, o en su defecto el encargado, garantizaran la seguridad de los datos, ya sea por medio de seudonimización y cifrado de datos personales; se garantizará la confidencialidad de los sistemas, y en caso de incidentes técnicos se deberá restaurar el acceso a los

datos. (pág. 51 y 52). Este es uno de los aspectos que en la práctica ha tenido más controversia, considerando que en septiembre del 2018 la multinacional Facebook anunció una falla en su seguridad que vulneró los datos personales de más de 50 millones de usuarios (Jara Sánchez, 2018).

Con respecto a las transferencias internacionales, en el artículo 44 (Parlamento Europeo y del Consejo, 2016, pág. 60) se estableció el principio general de transferencias, según el cual el traspaso de la información personal fuera del territorio europeo solo se llevará a cabo si el responsable cumple con el RGPD y de ese modo que pueda garantizarse el respeto a los derechos de los usuarios. La comisión decidirá si el tercer país o la organización garantizan un mínimo de derechos al proteger los datos personales. Según el artículo 46, (pág. 62) las organizaciones podrán hacer transferencia de datos sin el visto bueno de la comisión solo en caso de que ofrezca garantías mínimas de protección.

En definitiva, a pesar de que es un reglamento que puede llegar a tener vacíos, es contundente el esfuerzo de las autoridades europeas por otorgar herramientas a los usuarios de los datos personales que les permita obtener un verdadero poder sobre su información y ejercer debidamente sus derechos al limitar la libertad de las empresas que se encargan de operar con este tipo de información, por medio de la implantación de su responsabilidad materializada en la protección efectiva de datos sensibles personales.

En efecto, las organizaciones que utilicen la información personal al tener las obligaciones de establecer un trato legal, justificado y temporal usualmente por medio de la obtención de un consentimiento demostrable y libre; aunado al hecho de deber otorgar los denominados derechos ARCO, como son el acceso, rectificación, cancelación, oposición, limitación e inclusive la portabilidad de los datos personales, además de ejecutar acciones preventivas

a vulneraciones de derechos y libertades de personas naturales de acuerdo a la naturaleza de los datos y garantizar la seguridad a través de la implantación de medidas técnicas necesarias, entre otras obligaciones, tienen a su cargo varias cuestiones que no solo implican labores humanas, sino técnicas, organizativas y hasta económicas, imponiendo una carga mayor a la que usualmente acarrean.

Valdría la pena examinar cual ha sido el impacto efectivo en el ejercicio de las empresas, sobre todo de las mypimes europeas (como es el caso de las españolas que alojan sus datos -hosting- en Estados Unidos por los menores costos) quienes tuvieron varios reparos a la implementación del actual RGPD por sus altos costos y necesidades tecnológicas, además sería interesante determinar si como pretendieron el Parlamento y el Consejo de la Unión Europea en los considerandos del reglamento, se lograron levantar obstáculos a las transferencias internacionales de datos que a la postre redunda en el ejercicio del comercio internacional, o si por el contrario se impusieron más cargas que generan dificultades no para las multinacionales que tienen el capital suficiente para invertir en nuevas tecnologías y métodos para tratar datos sino para las nacientes empresas europeas.

II. ESTADOS UNIDOS DE NORTEAMÉRICA

En el otro extremo de la situación actual en materia de protección de datos personales, se encuentra el caso de Estados Unidos. Las políticas implementadas a nivel federal son sustancialmente diferentes a las europeas previamente examinadas, puesto que en esta federación se le dio prelación a otro tipo de principios que priman sobre la intimidad de los ciudadanos. En este país ha tenido mayor importancia los derechos de las empresas norteamericanas, puesto que en el ejercicio de prácticas mercantiles han tenido confianza en un principio determinante para el liberalismo económico que consiste en la auto regulación del mercado y la no necesidad de interferencia del gobierno por cualquier asunto.

Aunado a lo anterior, se encuentran diferencias sustanciales con el derecho europeo sobre la protección de datos, fundamentadas en una serie de razones históricas. Así lo explica Leonardo Cervera Navas en un artículo basado en la conferencia del 19 de julio de 2004 dictada en Madrid en el marco del Curso de Verano de El Escorial Presente y futuro de la protección de datos personales. Como primera medida vale la pena mencionar que, en desarrollo de la robusta protección estadounidense a las libertades y los derechos personales inculcada desde el nacimiento del estado norteamericano, el 15 de diciembre de 1890 se vislumbró por primera vez este tipo de problemáticas de manejo de datos por medio de la publicación del texto “the right to privacy” escrito por Samuel D. Warren y Louis D. Brandeis en la Harvard Law Review, donde se expresó que dentro de los principios del Common Law como son la propiedad privada existía un derecho a la privacidad, manifestado en “the right to be let alone” o derecho a que no molesten a un sujeto. En ese momento se violaron los derechos de las personas a no ser molestadas en su intimidad por medio de las fotografías instantáneas y periódicos. (Warren & Brandeis, 1890).

Ahora bien, a pesar del liderazgo en protección de datos personales en el siglo 19, explícitamente nunca se consagró el derecho en la constitución estadounidense ni en ninguna enmienda posterior. Como consecuencia, no hay desarrollo legal y debe extraerse de otros derechos del Common Law, a diferencia de Europa en donde se consagró en la Convención Europea de Derechos Humanos. En Estados Unidos "*el derecho a la protección de datos no se considera un civil right. En la tradición legal estadounidense se diferencian dos grandes categorías de derechos: los derechos civiles (civil rights) y las libertades públicas (civil liberties). El derecho a la protección de datos, que debería haberse caracterizado como un civil right en su origen, se presenta en realidad como una civil liberty, que además sería de naturaleza negativa: the right to be left alone. Las libertades públicas ceden más fácilmente frente a otros intereses que los derechos civiles*". (Cervera Navas, 2004, pág. 138). Aunado a lo anterior, se suma el hecho que políticamente no había tomado hasta ahora mucha relevancia el asunto de la protección de datos.

Es por lo anterior, que a nivel federal se ha limitado a unas cuantas leyes que tengan relación con los datos personales. En primer lugar, en 1996 se dictaminó la Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA por sus siglas en inglés), que tenía la finalidad de amparar la información de trabajadores y familiares que tuvieran alguna patología previa a obtener cobertura médica, circunstancia conocida como condición preexistente. (Sabatino, 2016). En segundo lugar, en 1998 se emitió la ley de Protección de la Privacidad Infantil en Internet (COPPA), cuya intención era proteger la información de menores de edad en internet, especialmente de menores de 13 años (Comisión Federal de Comercio, 2011). En tercer lugar, también en 1998 se proclamó el acta de protección de video privacidad según el cual se prohíbe a los establecimientos de renta de videos publicar sus clientes y sus rentas.

Finalmente, en 2003 se aprobó la Ley Federal de Transacciones Crediticias Imparciales y Exactas (FACTA), cuya finalidad era proteger información crediticia, e incluía aspectos como que en los recibos de transacciones no se podía incluir el número completo de cuentas, sino que debía limitarlo. (Prasse, 2009).

En cuanto a entidades públicas se emitieron dos disposiciones. La primera fue el Acta de privacidad en 1974, según el cual se establece un código de prácticas justas de recolección de información sobre ciudadanos que son recolectados por agencias federales. Para divulgar tal información debe constar el consentimiento del titular. El segundo es el acta de gobierno electrónico de 2002, en donde se dispuso que dados los cambios generados por los computadores y las redes digitalizadas se generan novedades para la protección de información comercial establecidos en registros del gobierno. Es por lo anterior que las entidades deben implementar nuevas tecnologías que traten información (ITA Bureau Privacy; Privacy, DOC Senior Agency Official for Officer).

No obstante, y considerando que el 24 de octubre de 1995 en Europa el Parlamento y el Consejo emitieron la Directiva 95/46/CE, por medio de la cual como se mencionó anteriormente se estableció un régimen legal relacionado con los datos personales garantista. Para establecer que el flujo de información personal siempre cumpliera los mínimos dispuestos en la Directiva, a las empresas europeas se les prohibió el flujo de datos personales a otros países fuera del continente que no cumplan los requisitos básicos de protección de datos personales (considerandos 56 y 57) (Parlamento Europeo y El Consejo de la Unión Europea, 1995). Empero, considerando que la transferencia de información personal a países extranjeros es tan relevante, estableció excepciones con el compromiso que aquellos terceros países cumplan las disposiciones de la Unión (considerandos 58, 59 y 60).

Es así como la Comisión de las Comunidades Europeas llegó a un acuerdo con el Departamento de Comercio norteamericano para adoptar la Decisión 2000/520 (La Comisión de las Comunidades Europeas, 2000), conocida como “Safe harbor” o puerto seguro en español. En este acuerdo se pretendió controlar el flujo de datos personales entre la Unión Europea y Estados Unidos por medio de una autocertificación de cumplimiento de la directiva del 95 por parte de las empresas norteamericanas. Las empresas extranjeras debían comprobar el cumplimiento de 7 los principios que determinarían que el manejo de los datos es siquiera similar al europeo. Tales principios son listados en la directiva europea, compuestos por la notificación, opción o consentimiento, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación. (pág. 5 y 6).

No obstante, la decisión 2000/520 fue anulada por el Tribunal de Justicia de la Unión Europea el 6 de octubre de 2015 en el caso “Max Schrems vs Facebook” por considerar que Estados Unidos efectivamente no garantizó un mínimo nivel de protección de los datos personales de europeos. Además, estimó que se vulneran los derechos establecidos en las disposiciones europeas cuando las entidades públicas, quienes no están en la obligación de cumplir con las normas de protección, tienen acceso indiscriminado a comunicaciones internacionales. Adicionalmente se infringe el derecho a la tutela judicial pues no hay mecanismos establecidos para que un titular de información solicite acceso, rectificación o supresión de sus datos generales. (Iuristec, 2015).

Por consiguiente, el 2 de febrero de 2016 la comisión europea y los Estados Unidos acordaron un nuevo “marco para los flujos transatlánticos de datos: el Escudo de la privacidad UE – EE.UU.”, por medio del cual efectivamente se protegieran los datos personales europeos transferidos a Norteamérica, dado que con fundamento en la decisión del Tribunal de Justicia Europeo nuevas exigencias se tendrían que requerir a las empresas norteamericanas que

recolectaran este tipo de información. Aunado a lo anterior, se estableció que el Departamento de Comercio y la Comisión Federal de Comercio norteamericanos debían jugar un papel más relevante e incluso cooperar con entidades europeas que protegen datos. Considerando que el asunto de acceso general sobre todo de entidades públicas norteamericanas a la información personal de millones de usuarios era uno de los mayores problemas con el "puerto seguro", se estipuló en este nuevo acuerdo que estos sujetos responsables del tratamiento de datos de ciudadanos europeos también tendrían limitaciones de acceso y serán sujeto de supervisión.

Adicionalmente, se plantearon más recursos para que los ciudadanos desde Europa soliciten sus reclamos o inquietudes y estos sean resueltos por las entidades estadounidenses en plazos establecidos con colaboración de las agencias de protección de datos europeas; la figura del mediador en Estados Unidos y la revisión anual del acuerdo entre los gobiernos. (European Comission Press Release DataBase, 2016). Formalmente, el "privacy shield" o el escudo de seguridad entró en vigencia el 1 de agosto de 2016.

Actualmente, esta institución está vigente, y consiste en un mecanismo de autocertificación de las empresas norteamericanas, que se realiza de forma virtual. Un total de 4925 organizaciones están activas y certificadas ante el Departamento de Comercio, mientras que 454 fueron certificadas y están inactivas. Los principios rectores irradiados por el RGPD son información, consentimiento, responsabilidad, seguridad, integridad y propósito, acceso, recursos y aplicación. Finalmente, en el acuerdo se incluyeron disposiciones sobre arbitramento obligatorio en caso de conflictos. (Privacy Shield Framework)

A raíz de la introducción del privacy shield y de la presión europea en cuestiones de protección de datos, numerosas empresas y estados de

Estados Unidos, empezaron a preocuparse por el establecimiento del RGPD y sus efectos en territorio trasatlántico. Es por lo anterior, que Estados como Arizona y Vermont han aprobado leyes que notifican en caso de brechas de seguridad y transparencia en el manejo de datos personales. Pero el aspecto más relevante, se dio el 28 de junio de 2018 fue firmada el Acta de Privacidad del Consumidor de California que entrará en vigor en el año 2020. A través de esta Acta, se busca otorgarles garantías a los titulares de información personal, notificando qué tipo de información almacenan, finalidades y además se otorga la posibilidad de prohibir la transferencia de tales datos, consolidándose como la Ley estatal más estricta sobre información personal de Estados Unidos, mencionando aspectos relacionados con el internet de las cosas. (Kelly, 2018).

Sin embargo, se han presentado varios casos de escándalos sobre la protección de datos en Estados Unidos, materializando de esa forma la preocupación especialmente europea. El primer evento se dio en junio de 2013, cuando Edward Snowden quien había trabajado como experto en seguridad informática para la Agencia Nacional de Seguridad (NSA) y la CIA informó al periódico inglés THE GUARDIAN (Greenwald, 2013) que el gobierno recaudaba registros telefónicos de usuarios de Verizon. El día siguiente, y siendo Snowden la fuente, el mismo diario expidió artículos donde se anunció sobre programas secretos que incluían vigilancia masiva secreta (PRISM) de la NSA. El PRISM es un sistema electrónico de vigilancia confidencial, especialmente de ciudadanos con domicilio fuera de los Estados Unidos. En este sistema vigilante se reúne todo tipo de información personal de los ciudadanos que interactúan por medio del internet. En respuesta el gobierno del momento respondió que se trataba de una herramienta poderosa que pretendía utilizarse para prevenir el terrorismo. Snowden manifestó que hizo público el programa con miras a que los derechos de libertad e intimidad

además de los datos personales de los titulares de la información personal fueran respetados.

En segundo lugar, en marzo de 2018, el diario The New York Times publicó un artículo donde afirmó que la consultora política Cambrigde analytica que trabajaba con campañas políticas "*extrajo información privada de los perfiles de Facebook de más de 50 millones de usuarios sin su consentimiento (…) lo cual dio como resultado una de las filtraciones más grandes de la historia de las redes sociales*" (Rosenberg, Confessore, & Cadwalladr, 2018). Tal situación empezó por medio de un test de personalidad denominado "This is your digital life", en 2013 difundido por medio de Facebook, que fue diligenciado por lo menos por 270.000 personas. A través de este test se recolectó la información personal de todos sus participantes y desde ahí se empezó a realizar perfiles de usuarios.

El tratamiento de la información privada de los ciudadanos norteamericanos permitió generar perfiles psicológicos de los usuarios de la red social, para de esa forma emitir publicidad e información que permitiera influir en la intención de voto de los votantes a favor del candidato Donald Trump en 2016, y se afirma que también a favor del brexit. El 2 de mayo de 2018 la empresa anunció su cese de actividades. Finalmente, y posterior a un año de investigaciones, en julio del presente año la Comisión Federal de Comercio de Estados Unidos (FTC) condenó a Facebook a una multa de US$5.000 millones como consecuencia de "malas prácticas" en la seguridad de la información de los usuarios tras haber filtrado sin consentimiento de los titulares información personal de aproximadamente 87 millones de usuarios con la empresa Cambridge Analytica.

Recientemente, Snowden afirmó que el gobierno de Estados Unidos no es el único que espía a las personas, sino que Facebook espía a todos sus usuarios.

Indicó que en las siguientes semanas explicará cómo redes sociales como Youtube, Instragram y Facebook espían a sus usuarios. (Morse, 2019).

En síntesis, la protección de la información personal en Estados Unidos es bastante cuestionable, considerando que en varias oportunidades empresas del mismo país han utilizado datos de millones de personas para ser tratados en Inglaterra por ejemplo, se han transferido datos de todo tipo e incluso mensajes personales para ejecutar análisis de las personas y se ha realizado test de personalidad como “This is your digital life” que fue diligenciado por lo menos por 270.000 personas a través de Facebook en 2013, para recolectar los datos personales con finalidades electorales y publicitarias.

No obstante, gracias a la política de intervencionismo limitado por parte del Estado de Estados Unidos, se ha permitido que sus empresas, hayan crecido hasta volverse los gigantes tecnológicos que tenemos hoy en día. Así que es necesario buscar un equilibrio entre estos dos extremos por medio de regulación, puesto que si bien el Estado está cimentado en principios fundamentales como son derechos individuales, gobierno limitado y derechos fundamentales como libertad, propiedad y derechos económicos, se ha vulnerado gravemente la intimidad de los ciudadanos norteamericanos al dar prevalencia absoluta a las compañías norteamericanas y haber permitido el acceso a la información personal de millones de ciudadanos y el tratamiento de tales datos sin como mínimo solicitar consentimiento, ni informar para qué se llevaría a cabo tal tratamiento ni quién lo haría ni mucho menos dar la oportunidad de rechazar tales operaciones. Como consecuencia, debe darse un mínimo de protección a la privacidad de las personas, como es el caso de los datos transferidos desde Europa con ocasión al “Privacy Shield”, según el cual se deben respetar estándares mínimos para poder tratar los datos de ciudadanos europeos.

III. COLOMBIA

En relación con el caso colombiano, se evidencia que ha tenido una marcada influencia europea en el desarrollo de la protección de los datos personales como derecho. En efecto, en el artículo 15 de la Constitución Política se consagró como derecho fundamental de la siguiente forma: "*todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre (…) De igual modo, tienen 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*. *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.*" (Asamblea Nacional Constituyente, 1991).

De ahí, se desarrolló una regulación rigurosa que incluye leyes y decretos, entre otros. La primera ley relacionada con el tema, fue la ley Estatutaria 1266 de 2008 que trata de datos personales financieros. En el 2009 con la ley 1273 se crearon nuevos tipos penales que están relacionado con delitos sobre la información y datos personales. En el 2014 entró en vigencia la Ley 1712 sobre el acceso a la información pública nacional. Finalmente, en el 2018 como consecuencia de la aprobación del Convenio sobre la ciberdelincuencia se emitió la Ley 1928.

Adicionalmente, con miras a ahondar en las anteriores leyes, se emitieron 4 Decretos, el 1727 de 2009 sobre información de los operadores de bancos, el 2952 de 2010 que reglamenta artículos de la ley 1266, el 1377 de 2013 por medio del cual se reglamenta la Ley 1581 y el 886 de 2014 que marca las pautas del registro nacional de bases de datos.

Sin embargo, en asuntos de datos personales, la principal Ley es la de “Habeas Data” número 1581 de 2012, que desarrolla el derecho constitucional consagrado en el artículo 15. Siguiendo los lineamientos europeos, dicha Ley en su artículo 2 rige la información personal de todas las bases de datos ya sean públicas o privadas, en el territorio del país o cuando el responsable no resida en territorio colombiano, pero deba cumplir con normas nacionales. Tiene exclusiones como información doméstica, información relacionada con la defensa nacional, prevención de delitos y periodística, entre otros. (Congreso de la República, 2012).

En su artículo cuarto, cita una serie de principios que irradian el tratamiento de datos personales, dentro de los cuales se incluye legalidad, finalidad legítima, libertad (que implica consentimiento informado del titular), veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. En su artículo 8, se plasmaron los conocidos derechos arco, consistentes en acceso, rectificación, cancelación y oposición al tratamiento de datos. El artículo 9 estipula la necesidad de brindar autorización para poder.

El responsable de tratamiento de los datos está obligado conforme al artículo 12 a avisar al titular de los datos sobre cuál será el tratamiento de sus datos y la finalidad del mismo, los derechos que tiene como titular y datos que permitan la identificación del responsable. En el artículo 17 se plasmaron las obligaciones de los responsables, que incluyen garantizar el ejercicio de los derechos de los titulares, almacenar autorización del titular, notificar sobre la finalidad del tratamiento de los datos, garantizar la seguridad para impedir acceso no autorizado, corregir inexactitudes de los datos, resolver consultas de los usuarios, notificar a la entidad encargada en casos de riesgos en las operaciones realizadas, entre otros.

Por medio del artículo 19 se le da la facultad a la Superintendencia de Industria y Comercio para ser la entidad encargada de vigilar el respeto de los principios y disposiciones de la Ley 1581 a través de una Delegatura para la protección de datos personales. En caso de incumplimiento a las disposiciones previstas, la Superintendencia tiene facultad de imponer sanciones a los infractores que van desde multas hasta por dos mil salarios mínimos mensuales legales vigentes, interrupción en el ejercicio de las operaciones con los datos, y cierre temporal o definitivo.

En Colombia también se incluyó el principio de Acountability o responsabilidad demostrada. En el artículo 26 del Decreto 1377 de 2013, el legislador colombiano impuso la obligación en cabeza de los responsables de los tratamientos de los datos personales de tener la capacidad técnica y probatoria de demostrar la implementación de medidas apropiadas para cumplir con los deberes de la Ley de habeas data del 2012

Finalmente, considerando que la Ley que despliega el Habeas Data establece unos mínimos a cumplir en el ejercicio de las operaciones con los datos personales, en su artículo 26 establece una prohibición de realizar traspaso de información a países que no cumplen con los derechos establecidos. Asimismo, establece excepciones de transferencias a países extranjeros que no cumplan con los mínimos de protección de datos personales, como en el caso de que el titular haya otorgado su consentimiento; verse sobre datos médicos; transferencias financieras; operaciones efectuadas a la luz de tratados firmados por el país; operaciones implicadas en el desarrollo de un contrato; operaciones para mantener el orden público o ejercicio de un proceso judicial.

Como consecuencia de lo anterior, para realizar operaciones con países que la Superintendencia considere que no hay una protección mínima, se deben

realizar más trámites ante tal entidad, para poder transferir los datos con la finalidad de obtener una Certificación de Conformidad. No obstante, los empresarios extranjeros pueden solicitar la autorización de los titulares de los datos para poder realizar el tratamiento, o cualquiera otra excepción mencionada anteriormente para poder transferir los datos, es decir que no es obligatoria la obtención del certificado de conformidad para poder tratar los datos de colombianos.

Para poder obtener tal certificado, el interesado por medio de una solicitud a la Superintendencia de Industria y Comercio debe informar nombre y finalidad del responsable y de sus bases de datos; tratamiento realizado a los datos personales; y si dentro de los datos tratados hay información sensible o de menores de edad; cuáles son las políticas de tratamiento; datos de identificación del responsable del tratamiento en el país a donde se transferirán los datos; documento que certifique existencia y representación legal del responsable extranjero; acuerdo o contrato donde se expresen los mecanismos y pormenores del tratamiento además de medidas de confidencialidad y seguridad; las operaciones y finalidades que realizará el responsable extranjero; políticas de tratamiento y de seguridad del responsable extranjero; mecanismos dispuestos para interponer consultas y reclamos del responsable extranjero; plazo de depósito de la información; copia de legislación sobre datos personales del país extranjero; igualmente copia de legislación donde se señale autoridad administrativa encargada de vigilar los tratamientos de datos personales además de herramientas que permitan denunciar o demandar la protección de derechos de titulares. (Superintendencia de Industria y Comercio, 2016).

Por medio de la sentencia C–748 de 2011 de la Corte Constitucional analizó la constitucionalidad de la Ley 1581 de 2012, y recalcó los parámetros generales para que la Superintendencia de Industria y Comercio determine si

un país receptor de datos personales de colombianos cumple con los mínimos requeridos de protección. Formuló que "(…) *un país cuenta con los elementos o estándares de garantía necesarios para garantizar un nivel adecuado de protección de datos personales, si su legislación cuenta; con unos principios, que abarquen las obligaciones y derechos de las partes (titular del dato, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos de datos personales), y de los datos (calidad del dato, seguridad técnica) y; con un procedimiento de protección de datos que involucre mecanismos y autoridades que efectivicen la protección de la información. De lo anterior se deriva que el país al que se transfiera los datos, no podrá proporcionar un nivel de protección inferior al contemplado en este cuerpo normativo que es objeto de estudio* (…)" (Pretelt Chaljub, 2011).

No obstante, vale la pena examinar el caso de la certificación colombiana a Estados Unidos en ejercicio de los artículos 21 y 26 de la Ley 1581, pues teniendo como base el escándalo denunciado por Snowden de filtración masiva de información personal de usuarios a nivel mundial, quedó claro que el régimen de protección de datos de Estados Unidos no es garantista de derechos. En ese sentido es menester recordar la sentencia del Tribunal de Justicia de la Unión Europa de 2015 por medio de la cual invalidó el acuerdo entre la UE con EEUU del "puerto seguro" por considerar que no se protegieron los datos de ciudadanos europeos en el país norteamericano. (Botero, 2017).

Sin embargo, por medio de la Circular Externa No. 005 del 10 de agosto de 2017[4] el Superintendente de la época, Pablo Felipe Robledo declaro que Estados Unidos cumplía con los mínimos de protección de datos personales. En borradores previos a la circular oficial, expedidos en julio, se incluyó a Estados Unidos como país que cumplía los requisitos para las empresas que

[4] Consultar en el Link: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Circular_Externa_5_Ago_10_2017.pdf

cumplían con la certificación emitida en el marco del acuerdo del “privacy Shield” entre Europa y Estados Unidos, pero no ante Colombia. Finalmente, en el texto final simplemente Estados Unidos apareció certificado por la Superintendencia sin un análisis de fondo. (Botero, 2017).

Ahora bien, a pesar que legalmente la Superintendencia De Industria y Comercio debe establecer con fundamento en unos criterios determinados si el país receptor de los datos personales cumple con mínimos establecidos en la Ley 1581, queda un gran interrogante sobre la certificación de Estados Unidos, pues empezando por el hecho que no existe una Ley federal ni una autoridad central que obligue a los responsables del manejo de los datos a salvaguardar los derechos de los titulares, aunado a las denuncias de los malos manejos de empresas norteamericanas de la información personal de usuarios alrededor de todo el mundo, se puede concluir que la autoridad administrativa Colombiana sin haber fundamentado de fondo la resolución de otorgar el certificado de conformidad a Estados Unidos no tomó la mejor decisión; y por el contrario, considerando la importancia en el mercado de las empresas tecnológicas estadounidenses, recomendar la implantación de mecanismos de autocertificación similares al “privacy shield” o acuerdos de cooperación entre los dos países hubiera sido la solución más garantista para salvaguardar la información de los ciudadanos colombianos que es procesada en Estados Unidos.

Por otro lado, y más recientemente con el cambio de gobierno, en consonancia con los escándalos internacionales de Facebook relacionados con los datos personales de sus usuarios, por medio de la resolución 1321 de 2019 del 24 de enero, la Superintendencia de Industria y Comercio emitió directrices preventivas a Facebook para garantizar la seguridad del manejo de los datos de los usuarios colombianos y la responsabilidad demostrada, teniendo en cuenta las manifestaciones de medios de comunicación y autoridades de protección de datos personales sobre el caso de Cambridge Analytica, hurto de tokens para entrar a las cuentas de usuarios y acceso injusto a fotografías,

y considerando que Facebook tiene información de más de 31 millones de colombianos, es decir aproximadamente el 68% de información de los colombianos que además, transfiere a otros países. (Superintendencia de Industria y Comercio, 2019)

En definitiva, con fundamento en estadísticas de la autoridad administrativa Colombiana -la Superintendencia de Industria y Comercio- sobre un aumento del 34% en el 2018 de las quejas de los usuarios por infracciones a los deberes del habeas data, conformadas por un número de 900 quejas mensuales y que se tradujeron en sanciones a 71 responsables y multas por 5.600 millones de pesos por infracciones a sus deberes (Olaya, 2019), se pueden concluir varias situaciones en Colombia.

En primera medida, y partiendo de la base que en lo transcurrido del presente año solo han investigado a dos empresas extranjeras, y que por lo tanto el grueso de empresas investigadas son colombianas, se puede afirmar que estos derechos cada vez son más conocidos por los ciudadanos y que los mecanismos dispuestos en el país para que los usuarios puedan exigir el cumplimiento de sus derechos funcionan debidamente a nivel nacional.

En segunda medida, la disposición legal del certificado de conformidad de cumplimiento de estándares mínimos de protección a los derechos derivados de los datos personales es una buena medida para determinar y vigilar la transferencia de la información personal de colombianos a terceros países, esto permite ejecutar un análisis previo y determinar qué tipo de riesgo conlleva permitir la transmisión de información personal de usuarios colombianos.

No obstante, vale la pena resaltar la infortunada revisión a los estándares de protección de Estados Unidos, pues se le otorgó el certificado de conformidad sin cumplir varias de las disposiciones establecidas en la Ley 1581 de 2012, motivo por el cual vale la pena revisar si efectivamente las empresas

norteamericanas salvaguardan los derechos de los ciudadanos colombianos sobre sus datos personales que son transferidos para ser tratados en el país norteamericano y en caso de no cumplir el piso garantista colombiano tomar las medidas pertinentes para no afectar el comercio entre países pero tampoco vulnerar los derechos de los colombianos.

En otras palabras, conforme a las realidades actuales del mercado que se traducen en una transferencia de datos personales a nivel mundial para variados fines como mercadeo, publicidad y comercialización entre otros, como medida de facilitar mecanismos para garantizar el cumplimiento de deberes relacionados con los datos personales, la instauración de mecanismos de cooperación entre autoridades administrativas encargadas de velar por los derechos de los usuarios a nivel mundial constituiría una medida acertada y pertinente con miras a otorgar herramientas con un alcance más completo a los ciudadanos colombianos, es decir que implementar acuerdos con disposiciones similares a las de colaboración administrativa del “privacy shield” con países que más acceden a la información de los colombianos, permitiría una mayor protección de sus derechos.

A continuación, se resumen los aspectos más relevantes que determinan las grandes diferencias entre los regímenes europeo, colombiano y estadounidense. Entre tales ítems, se incluyen temas como sanciones, ámbito legal, autoridad central y alcance.

Resumen estándares de protección de datos personales

Régimen	**Ámbito Legal**	**Autoridad Central**	**Alcance**	**Enfoque**	**Sanciones**
Europa	RGPD Todo Europa	Agencias Nacionales, Grupo UE Directiva	General con excepciones literales	Preventivo/Estatal. Derecho Fundamental	RGPD
Colombia	Ley 1581/12 Todo el país	SIC	General con excepciones	Preventivo/estatal. Derecho Fundamental	Ley 1581/12

EEUU	Normativa sectorial, no Ley federal	Departamento de Comercio y la Comisión Federal de Comercio Cooperan en el “privacy Shield”, pero entidad oficial para protección general no existe.	Particular, caso a caso en tribunales	Resolutivo/mercado, ante los tribunales. Derecho accesorio.	Determinadas por tribunales en el caso a caso

IV. LA REVOLUCIÓN DIGITAL, EN PARTICULAR EL MACHINE LEARNING Y EL INTERNET DE LAS COSAS FRENTE A LA PROTECCIÓN DE DATOS PERSONALES

Ahora bien, considerando que nos encontramos en medio de la cuarta revolución industrial, denominada revolución digital, y que los datos son los activos más importantes para las empresas, cada vez es más común encontrar en la cotidianidad el uso de "nuevas tecnologías"[5] que permiten procesar grandes cantidades de datos para establecer decisiones, pues es posible determinar comportamientos de sujetos. Es así como cada vez más empresas (sobre todo de venta de productos) a nivel mundial pueden conocer preferencias de sus clientes y de tal forma reducir los riesgos inherentes de los negocios. Luego el análisis de la información está cambiando las industrias, pues en sectores como las ventas al por menor los hábitos de consumo, gustos y predicciones de los consumidores están siendo establecidas con fundamento en el uso de herramientas como el big data o el learning machine. (Barquin, 2019).

En particular, la inteligencia artificial tiene un arraigo distinguido en nuestras vidas por medio de aplicaciones en el celular, como por ejemplo utilización de reconocimiento facial, asistentes virtuales de voz y recomendaciones en aplicaciones como Netflix y de venta de productos. Es entendida como "*la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano."* (Iberdrola).

[5] Como son el internet de las cosas, la nube, la cadena de bloques, la inteligencia artificial, la analítica predictiva, el big data, minería de datos y la automatización robótica de procesos, entre otros.

Una de las ramas más notables que se ha derivado de la inteligencia artificial, es el learning machine, o aprendizaje automatizado; consiste en una técnica para analizar los datos con la finalidad de construir modelos analíticos de forma eficiente, para identificar patrones y de esa forma tomar decisiones. Específicamente, en industrias bancarias para prevenir el fraude, el gobierno para hacer más efectiva la medición de datos de servicios públicos, evaluación de síntomas médicos de pacientes, ventas por medio de la recomendación de productos, eficiencia en las rutas de la industria de transporte e incluso en el sector petrolero el aprendizaje automatizado cada vez tiene un papel más importante. (SAS).

Sin embargo, estas nuevas técnicas lo que hacen es recaudar y tratar datos que, en muchas oportunidades son datos personales de usuarios alrededor del mundo, situación que es preocupante considerando la creciente cantidad de datos recolectados a nivel global. En efecto, según estudios para el año 2020 se prevé que serán 44 zettabytes o 44 trillones de gigabytes de datos mundiales, pues actualmente se envían aproximadamente 500.000 trinos por Twitter por minuto, 180 millones de correos y por medio de Google se realizan cerca de 3,7 millones de búsquedas. (Eres, 2019).

Otra herramienta cada vez más implementada en los hogares mundiales a través de marcapasos en pacientes con complicaciones cardiacas, biochip de animales, sensores de presión baja de las llantas en los carros, entre otros; es el internet de las cosas, considerada como un *“sistema de dispositivos de computación interrelacionados, máquinas mecánicas y digitales, objetos, animales o personas que tienen identificadores únicos y la capacidad de transferir datos a través de una red, sin requerir de interacciones humano a humano o humano a computadora.”* (Rouse, 2017).

Empero, herramientas como las mencionadas facilitan a los hackers la filtración de datos de usuarios, pues por medio del aprendizaje automatizado atacan masivamente bases de datos. En concreto, todas las infracciones a la protección de los datos personales comienzan con su recopilación, los hackers clasifican usuarios y seleccionan víctimas. También utilizan la suplantación de identidad por medio de correo no deseado para extraer información personal. Tales actividades se pueden desarrollar por medio del aprendizaje automatizado. (Polyakov, 2018)

Precisamente el Foro Económico Mundial ha concluido que los ataques cibernéticos y el fraude de los datos son los riesgos globales más probables en nuestros tiempos. En Europa con la implementación del RGPD se ha conformado un cimiento legal fuerte para proteger los derechos de los europeos, y en Estados Unidos a penas el estado de California emitió un acto que regula el internet de las cosas. (Gravrock, 2019).

De modo que, la OCDE[6] emitió “el primer conjunto de directrices de políticas intergubernamentales sobre inteligencia artificial (IA) con miras a evitar la incursión en abusos por parte de empresarios que lo utilizan para generar conocimiento de los datos personales recogidos. Naturalmente, los países miembros (36 en total) además de otros como Colombia, Brasil, Perú y Costa Rica suscribieron tales directrices que deberían permear las realidades en el mercado. Se incluyeron principios relacionados con la confianza de la inteligencia artificial, dentro de los cuales se mencionó finalidad del uso, por medio de servicio a las personas; respeto a los derechos fundamentales; transparencia y divulgación responsable; seguridad y gestión de riesgos; y responsabilidad demostrada. (OCDE, 2019).

[6] Organismo que siempre está a la vanguardia de las realidades económicas de los países. Tales principios de IA se fundamentaron en Directrices de la Comisión Europea.

Así las cosas, y evidenciando que cada vez más se hacen recolecciones masivas de datos personales, para ser tratados por medio de algoritmos automatizados, la aplicación de los principios sugeridos por la OCDE toma un papel protagónico, pues al ser estos mecanismos cada vez más comunes, es necesario con fundamento en los principios de transparencia y finalidad, informar a los usuarios sobre las características del tratamiento de sus datos para que de esa forma puedan ejercer debidamente sus derechos.

En consonancia con lo anterior, no solo debe brindarse un catálogo de derechos a los consumidores en la web, sino que debe en verdad reflejarse en el ejercicio de la cotidianidad. Por ejemplo, cuando un usuario debe brindar sus datos personales como moneda de cambio para acceder a una aplicación en sus dispositivos móviles o a una página web, la única forma que tiene para poder entrar es acceder a las políticas de seguridad y privacidad o suministrando datos, pero si el usuario no quiere aceptar entonces se le niega el acceso. Otros ejemplos consisten en la necesidad de brindar la ubicación geográfica, registro o creación de alguna cuenta o aceptar políticas de cookies para poder acceder a sitios web o aplicaciones. Es por lo anterior, que debe revisarse el ejercicio del consentimiento por parte de los usuarios pues este necesita en verdad ser libre y no solo verse forzado a aceptar unas condiciones para poder acceder a información o servicios. (Sinrod, 2018)

No obstante, la solución no debe fundamentarse solo en regulación estatal, pues esta es solo una de las piezas claves del rompecabezas de los datos personales. Debe estar integrado también por políticas implantadas por las empresas tecnológicas, pues deben tratar los datos que los ciudadanos les brindan por medio del internet como el ejercicio de un derecho fundamental. Esta cuestión es complicada teniendo en cuenta las estructuras de negocios y las formas como la mayoría de empresas tecnológicas emplean la información de los usuarios, pero es un asunto a manejar para poder efectivamente

atender la necesidad de proteger los datos personales de consumidores a nivel global.

Como una tercera medida, también es mandatorio el auto control de cada ciudadano al navegar por la web, es decir que, el usuario al ser el encargado de determinar cuáles son los datos que está dispuesto a intercambiar como moneda de cambio para tener como contraprestación contenidos digitales o servicios, y si vale la pena acceder a las políticas de privacidad brindadas en internet, debe llegar a entender lo que implica aceptar los términos y condiciones impuestos sin prestar mayor atención, y debe adoptar precauciones frente a las políticas impuestas digitalmente. (Sinrod, 2018) (Jiménez & Coronado, 2017). Esto implicaría el ejercicio de campañas de concientización que deberían estar en cabeza de las autoridades administrativas de cada país, como sería el caso de la Superintendencia de Industria y Comercio en Colombia. Igualmente, los medios de comunicación, como pretende hacerlo Edward Snowden, podrían divulgar los verdaderos alcances que tienen el manejo de nuestros datos personales por internet.

CONCLUSIONES

En definitiva, para buscar un balance entre el ejercicio del comercio internacional y la protección de los datos personales de los consumidores debe ajustarse las regulaciones a nivel global, para que se acerquen cada vez más al estándar garantista de la Unión Europea e implementar los principios sobre Inteligencia Artificial.

Pero en aquellos países donde sean arduas las negociaciones se podría implementar una herramienta similar al “privacy shield” instaurado entre Estados Unidos y Europa, sin importar que tenga falencias y vacíos, puesto que es el mecanismo que más está cercano a verificar de cerca y otorgar vías de acceso y reclamo a los consumidores el ejercicio del derecho a la protección de sus datos.

Es así como en Colombia debe revisarse el ejercicio de la protección de datos especialmente con empresas norteamericanas considerando la dudosa certificación otorgada por el Superintendente de Industria y Comercio según la cual supuestamente se garantiza el cumplimiento de la Ley 1581 de 2012. En este sentido la implementación de una plataforma virtual de autocertificación por parte de la Superintendencia de Industria y Comercio para poder garantizar los derechos de los ciudadanos colombianos es una medida pertinente que permitiría materialmente proteger la información de los colombianos que es tratada fuera del país.

También debe buscarse la cooperación de las empresas tecnológicas, incluidas las gigantes como Google y Facebook para que materialmente garanticen los derechos de los consumidores e informen todo respecto del tratamiento de la información. Y finalmente, se hace necesario proseguir con la reducción de asimetrías de información sobre los consumidores y de esta

forma informarlos sobre las consecuencias de otorgar sus datos sin tener conciencia sobre para qué los van a usar.

BIBLIOGRAFÍA

DOCUMENTOS ELECTRÓNICOS

Asamblea Nacional Constituyente. (1991). Secretaría de Senado. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Barquin, R. (13 de mayo de 2019). Computer world colombia. Obtenido de https://computerworld.co/los-datos-el-nuevo-oro-digital/

Botero, C. (16 de agosto de 2017). La silla vacia. Obtenido de https://lasillavacia.com/silla-llena/red-de-la-innovacion/historia/chanfle-colombia-declaro-adecuada-la-proteccion-de-datos

Cervera Navas, L. (19 de julio de 2004). El modelo europeo de protección. Obtenido de * Artículo basado en la conferencia pronunciada en el Curso de Verano de El Escorial Presente y futuro de la protección de datos personales, Madrid, 19 de julio de 2004.: https://core.ac.uk/download/pdf/61482450.pdf

Comisión Federal de Comercio. (septiembre de 2011). Comisión Federal de comercio. Obtenido de Información para consumidores: https://www.consumidor.ftc.gov/articulos/s0031-como-proteger-la-privacidad-de-su-hijo-en-internet

Congreso de la República. (octubre de 18 de 2012). Secretaría de senado. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Consejo de Europa. (28 de enero de 1981). Obervatorio Ciro Angarita Barón sobre la protección de datos personales en colombia. Obtenido de Universidad de los Andes: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Convenio108-19811.pdf

Cuesta, M. (21 de mayo de 2019). ABC economia. Obtenido de https://www.abc.es/economia/abci-google-facebook-amazon-y-apple-tienen-poder-absoluto-informacion-digital-201711260206_noticia.html

Eres, C. (21 de mayo de 2019). linkedin. Obtenido de https://www.linkedin.com/pulse/el-oro-de-la-era-digital-los-datos-carlos-eres/

European Comission Press Release DataBase. (2 de febrero de 2016). Comisión europea. Obtenido de http://europa.eu/rapid/press-release_IP-16-216_es.htm

FXSSI. (13 de enero de 2019). FXSSI. Obtenido de https://es.fxssi.com/las-empresas-mas-valiosas-del-mundo

Gil, R. (30 de mayo de 2019). trend tic tendencias tecnológicas & negocios. Obtenido de https://www.trendtic.cl/2019/05/los-datos-son-el-nuevo-oro-gobernarlos-es-la-clave-del-exito/

Gravrock, E. V. (8 de enero de 2019). World Economic Forum. Obtenido de World Economic Forum: https://www.weforum.org/agenda/2019/01/who-should-take-charge-of-our-cybersecurity/

Greenwald, G. (6 de junio de 2013). The guardian. Obtenido de https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Iberdrola. (s.f.). Iberdrola. Obtenido de https://www.iberdrola.com/innovacion/que-es-inteligencia-artificial

ITA Bureau Privacy; Privacy, DOC Senior Agency Official for Officer. (s.f.). privacy shield framework. Obtenido de https://www.privacyshield.gov/Website-Privacy-Policy

Iuristec. (4 de diciembre de 2015). ¿Que es “Safe Harbor”?: Implicaciones de la anulación de este acuerdo. Obtenido de Iuristec: http://www.iuristec.es/?p=6727

Jara Sánchez, G. (16 de octubre de 2018). RGDP blog. Obtenido de http://rgpdblog.com/quiebra-de-seguridad-de-datos-personales-en-facebook-la-primera-gran-infraccion-del-rgpd/

Jiménez Pacheco, M. N., & Leal Coronado, M. (junio de 2017). Centro de Estudios de Consumo CESCO. Obtenido de http://centrodeestudiosdeconsumo.com/images/Contenidos_digitales_e_intercambio_datos.pdf

Kelly, H. (30 de junio de 2018). California aprueba la ley de privacidad en internet más estricta de Estados Unidos. Obtenido de cnn: https://cnnespanol.cnn.com/2018/06/30/california-ley-privacidad-internet-estricta-estados-unidos/

La Comisión de las Comunidades Europeas. (26 de julio de 2000). 2000/520/CE. Obtenido de eur.lex: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0520&from=ES

Lopp, C. A. (20 de abril de 2017). Obtenido de http://blogs.eltiempo.com/huella-forense/2017/04/20/abc-del-habeas-data-ley-1581-del-2012/

Morse, J. (1 de agosto de 2019). Mashable. Obtenido de technology: https://mashable.com/article/edward-snowden-facebook-instagram-spying/

Naciones Unidas. (14 de diciembre de 1990). Página Principal de las Naciones Unidas. Obtenido de RESOLUCIONES APROBADAS POR LA ASAMBLEA GENERAL DURANTE EL 45° PERÍODO DE SESIONES: https://www.un.org/es/documents/ag/res/45/list45.htm

NEWS, B. (24 de julio de 2019). BBC NEWS. Obtenido de https://www.bbc.com/mundo/noticias-49093124

OCDE. (2002). Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Obtenido de https://www.oecd.org/sti/ieconomy/15590267.pdf

OCDE. (2018). OCDE mejores políticas para una vida mejor. Obtenido de https://www.oecd.org/centrodemexico/laocde/

OCDE. (22 de mayo de 2019). OCDE. Obtenido de https://www.oecd.org/centrodemexico/medios/cuarentaydospaisesadoptanlosprincipiosdelaocdesobreinteligenciaartificial.htm

Olaya, M. (30 de enero de 2019). RCN RADIO. Obtenido de https://www.rcnradio.com/colombia/mas-de-900-quejas-se-reciben-al-mes-por-violacion-de-datos-personales

Oliveira, J. (26 de junio de 2018). Openmind. Obtenido de https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/los-5-mandamientos-de-la-inteligencia-artificial/

Parlamento Europeo y Consejo de la Unión Europea. (4 de mayo de 2016). Diario oficial de la unión europea. Obtenido de Reglamento General de Protección de Datos: https://www.boe.es/doue/2016/119/L00001000088.pdf

Parlamento Europeo y del Consejo. (04 de 05 de 2016). rgpd. Obtenido de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Parlamento Europeo y El Consejo de la Unión Europea. (24 de octubre de 1995). Obtenido de Diario Oficial n° L 281 de 23/11/1995 p. 0031 - 0050: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

Perasso, V. (12 de octubre de 2016). BBC. Obtenido de BBC: https://www.bbc.com/mundo/noticias-37631834

Polyakov, A. (11 de enero de 2018). forbes. Obtenido de https://www.forbes.com/sites/forbestechcouncil/2018/01/11/seven-ways-cybercriminals-can-use-machine-learning/

Prasse, E. (2009). Extensión de la Universidad de Illinois. Obtenido de Consejos utiles para el uso de las tarjetas de credito: https://extension.illinois.edu/creditcardsmarts_sp/Fair_accurate_credit_transaction_act.cfm?2

Pretelt Chaljub, J. I. (6 de octubre de 2011). Corte Constitucional República de Colombia. Obtenido de http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Privacy Shield Framework. (s.f.). Privacy shield framework. Obtenido de https://www.privacyshield.gov/welcome

Remolina Angarita, N., & Alvarez Zuluaga, L. F. (junio de 2018). Observatorio Ciro Angarita Barón GECTI sobre la protección de datos personales. (U. d. andes, Ed.) Obtenido de Universidad de los andes: https://gecti.uniandes.edu.co/index.php/accountability

Remolina Angarita, N., Tenorio Adame, M. M., & Quintero Navas, G. A. (2018). De la Responsabilidad demostrada en las Funciones Misionales de la Registraduria Nacional del Estado Civil. Bogotá: Temis. Recuperado el 3 de junio de 2019, de https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/De-la-responsabilidad-demostrada-en-las-funciones-de-la-RNEC-2018-Nelson-Remolina-Angarita1.pdf

Rosenberg, M., Confessore, N., & Cadwalladr, C. (20 de marzo de 2018). New York Times. Obtenido de https://www.nytimes.com/es/2018/03/20/cambridge-analytica-facebook/

Rouse, M. (enero de 2017). Techtarget. Obtenido de https://searchdatacenter.techtarget.com/es/definicion/Internet-de-las-cosas-IoT

Sabatino, C. (junio de 2016). Manual Merck. Obtenido de https://www.merckmanuals.com/es-us/hogar/fundamentos/asuntos-legales-y-%C3%A9ticos/la-confidencialidad-y-la-hipaa-ley-de-portabilidad-y-responsabilidad-de-seguros-de-salud-en-estados-unidos

SAS. (s.f.). SAS The Power to Know. Obtenido de https://www.sas.com/es_co/insights/analytics/machine-learning.html

Sinrod, M. L. (23 de mayo de 2018). World Economic Forum. Obtenido de World Economic Forum: https://www.weforum.org/agenda/2018/05/GDPR-personal-data-privacy-regulation/

Superintendencia de Industria y Comercio. (2016). Superintendencia de Industria y Comercio. Obtenido de Delegatura de Protección de Datos: http://www.sic.gov.co/centro-de-publicaciones?field_tema_general_tid=5&field_anos_p_value=All

Superintendencia de Industria y Comercio. (24 de enero de 2019). Superintendencia de Industria y Comercio. Obtenido de Delegatura Protección de Datos Personales: http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/Res-1321-de-2019(1).pdf

Warren, S. D., & Brandeis, L. D. (15 de diciembre de 1890). Harvard Law Review, Vol. 4, No. 5. pp. 193-220. Obtenido de JSTOR: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf