LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES UNA PRÁCTICA EFECTIVAMENTE CONTROLADA O UTÓPICAMENTE REGULADA

NATALY HOYOS GÓMEZ

UNIVERSIDAD EAFIT

FACULTAD DE DERECHO

ESCUELA DE DERECHO

MEDELLÍN

2017

LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES UNA PRÁCTICA EFECTIVAMENTE CONTROLADA O UTÓPICAMENTE REGULADA

NATALY HOYOS GÓMEZ

Trabajo de grado para optar al título de Abogado

Asesor:

Mónica Restrepo

UNIVERSIDAD EAFIT

FACULTAD DE DERECHO

ESCUELA DE DERECHO

MEDELLÍN

2017

Nota de Aceptación

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Medellín, Octubre de 2017

La transferencia internacional de datos personales una práctica efectivamente controlada o utópicamente regulada

RESUMEN

Con el surgimiento de nuevas vías de comunicación, los datos personales se han convertido en un bien permanentemente comercializado a nivel internacional, cobrando mayor relevancia social y económica debido a que son uno de los mayores insumos necesarios para el funcionamiento de las sociedades modernas, la construcción y mantenimiento de relaciones comerciales y personales propias de la globalización.

La comercialización de los datos personales fuera del país de origen, llamada transferencia internacional de datos, se constituye efectivamente cuando el responsable y/o encargado del tratamiento de los datos[1], envía información o bases de datos a un receptor, que a su vez es responsable del tratamiento y se encuentra fuera del país. En las etapas de cesión y cruce de información, la transferencia internacional de datos deja como resultado la disposición de datos a millares de usuarios dispersos geográficamente.

El tránsito internacional de datos exige una normatividad de carácter global, que permita la protección de los derechos humanos y las libertades fundamentales, sin importar el país de origen o destino de los datos personales.

En el desarrollo del artículo se evidenciaron grandes dificultades, una de ellas es que los titulares de los datos, aun cuando están facultados de mecanismos de protección e información ofrecidos por los países de origen de sus datos, no pueden llegar a tener un verdadero control de su información cuando traspasan las fronteras nacionales.

Es muy común hablar del "nivel adecuado" de protección de datos necesario en los países receptores para que sea posible la transferencia de datos personales del país de origen. Sin embargo, los grandes modelos como el de la Unión Europea y Estados Unidos de América han demostrado que esto no es suficiente, es necesario que entre los países se efectúen acuerdos que permitan que las normas de protección de los datos personales sean vinculantes a los titulares de los datos que se encuentran fuera del país receptor.

[1] Se tienen en cuenta las definiciones de Responsable y encargado establecidas en la ley 1581 de 2012 Art. 3, reglamentada parcialmente por el decreto 1377 de 2013.

En Colombia aún no se cuenta con la regulación de régimen de puerto seguro, como la establecida mediante acuerdos entre la UE y EE.UU. Colombia escasamente esta adicionando un capítulo a la Circular Única de la Superintendencia de Industria y Comercio, con relación a la transferencia internacional de datos personales en la que se fijan los estándares de un nivel adecuado de protección en el país receptor de la información personal y las condiciones para obtener una declaración de conformidad.

Por lo anterior, declarar que un país tiene un nivel adecuado de protección de datos no es suficiente para garantizar la protección efectiva de los derechos de los titulares cuando se efectúan las trasferencias internacionales, llevando a la conclusión de que los vacíos normativos a nivel internacional, en la regulación de las transferencias de datos, son evidentes y se hace necesario adoptar acuerdos entre Colombia y países receptores que permitan, aun cuando sus normativas no son iguales, una posible vinculación entre éstas para los datos transferidos, llevando a que el titular tenga mecanismos de protección internacional y no solo nacional, manteniendo el control de sus datos y el tratamiento que se le da a los mismos a nivel internacional.

Palabras Claves: Datos personales, transferencia, titular, Responsable, Encargado, Datos sensibles, Privacidad, información, Protección de datos, Tratamiento, Autorización, Intimidad, Modelo Europeo, Modelo Norteamericano, Modelo Híbrido, Circulación, Garantías, Seguridad, Comisión Europea, Autorización, Contratos.

INTRODUCCIÓN

El presente trabajo pretende efectuar un análisis de la transferencia internacional de datos personales, que permita evidenciar la ineficacia de la normatividad Colombiana para la protección de los titulares de los datos personales cuando se efectúa una transferencia internacional, perdiendo validez al sobrepasar el ámbito espacial, temporal, material y personal de la normatividad nacional.

El derecho de *Habeas Data* o *autodeterminación informática* (Sentencia T - 058, 2015)[2] ha sido la respuesta que históricamente se le ha dado al poder informático en la esfera internacional de los derechos humanos y del derecho constitucional como *"Dominio social sobre el individuo*", y consistente en "La *posibilidad de acumular información en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerle seguimiento en una memoria indefectible, de objetivarlas y transmitirlas como mercancía*". (Sentencia T - 058, 2015)

La Declaración Universal de los Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los derechos civiles y políticos protege los derechos que se derivan del Habeas Data, tales como la libertad individual, la libertad de expresión, la intimidad y la dignidad personal, declarando que "*nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación*".

[2] La Corte Constitucional señalo que "[u]n derecho fundamental autónomo que tiene la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquél que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo".

En Colombia, el derecho de Habeas Data está expresamente regulado en el Art. 15 de la Constitución Política de 1991, en el cual después de consagrar los derechos a la intimidad y al buen nombre, agrega que las personas: *"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*".

El objeto de protección de estos derechos, es el "dato personal", es decir, toda aquella información relativa a los sujetos que lo identifican o permiten identificarlo, que lo describen, precisan su origen, edad, referencia de domicilio o residencia, trayectoria académica, laboral o profesional; y lo referente a aspectos más sensibles o delicados como la forma de pensar, estado de salud, características físicas, ideologías o vida sexual.

Al derecho de protección de datos lo componen dos dimensiones; por un lado, le confiere al titular de los datos el poder jurídico para conocer e incidir sobre el contenido y la difusión de los mismos; y por otro lado, instaura un conjunto de directrices a partir de las cuales, los responsables de las bases de datos, deben proteger los datos en sus etapas de recolección, tratamiento, cesión y cruce de información. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

Con la expedición de la ley 1266 de 2008, se dio inicio a la regulación del Habeas Data en aspectos financieros, pero solo hasta el 2012 con la expedición de la ley 1581 se reguló en su art. 26[3] la transferencia internacional de datos personales, estableciendo como regla general

[3] El artículo 26 de la Ley 1581 de 2012 establece que: "Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.
Esta prohibición no regirá cuando se trate de:

la prohibición de transferir datos personales de cualquier tipo a países que no proporcionen "Niveles adecuados de protección" de datos. "*Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, las cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios"* (Circular externa 005, 2017), haciendo necesario establecer estándares que permitan determinar qué países cuentan con un nivel adecuado de protección de datos personales.

Hay una transferencia internacional, cuando los datos efectivamente salen del territorio colombiano. " *La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país*". (Decreto 1377 , 2013)

Dicha transferencia se da en las etapas de recolección y/o cesión o cruce de la información, haciendo necesario el consentimiento o autorización del titular para la transferencia, con el fin de evitar sobrepasar la esfera de la privacidad y lesionar los derechos y libertades del

---

a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;
b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;
c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;
d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;
e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;
f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
Parágrafo 1°. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.
Parágrafo 2°. Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008."

mismo, generando la necesidad de establecer el equilibro entre el individuo y las organizaciones públicas y privadas que recolectan y utilizan datos, por medio de la regulación y protección.

Con la expedición del decreto 1377 de 2013, se dictaron disposiciones generales para la protección de datos personales y se facultó a la Superintendencia de Industria y Comercio para ejercer la vigilancia y protección de los derechos, garantías y procedimientos de la ley. Sin embrago, solo hasta la Circular N° 5 la Superintendencia de Industria y Comercio fija los estándares de un nivel adecuado de protección en los países receptores de la información personal y las condiciones para obtener una declaración de conformidad, para realizar transferencias internacionales de los datos personales de los Colombianos a terceros países.

En la Unión Europea la primera norma que marcó las pautas del modelo de protección de datos fue el convenio N° 108 del Consejo de Europa, aprobado en 1981, del cual surgieron luego las recomendaciones de la OCDE sobre los principios relativos a la protección de la privacidad y la transferencia internacional de datos personales. (Cuadrada, 2007)

En el año 1995, el Parlamento y el Consejo, confeccionaron la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En el 2000 con apoyo del art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, documento por el cual se reafirman los derechos reconocidos por las tradiciones constitucionales y las obligaciones internacionales comunes de los Estados miembros, se reconoce explícitamente el derecho a la protección de los datos de carácter personal. Sin embargo, para el año 2016 como consecuencia de la rápida evolución tecnológica y la necesidad de dar uniformidad al régimen jurídico en materia de

protección de datos entre los estados miembros, el parlamento Europeo adoptó el proyecto de reglamento general de protección de datos, este reglamento 2016/619, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, ha sustituido a la Directiva 95/46/CE. (Vicente Guasch Portas, 2014)

En Estados Unidos (EE.UU), la protección de la privacidad ha evolucionado de una manera diferente, al ser un estado federal integrado por 50 estados y distritos[4], la privacidad puede hallarse regulada tanto por la federación como por cada uno de sus estados miembros. Bajo una mirada internacional EE.UU ratificó las directrices sobre protección de la vida emitida por la OCDE en 1980. No obstante, la protección de la privacidad debe revisarse desde dos ámbitos, uno público y otro privado. En la quinta y cuarta enmienda de la constitución de EE.UU, su reconocimiento constitucional solo fue dirigido al sector público y recoge el derecho del individuo a la seguridad de su persona, de su domicilio, papeles y efectos, contra registros e incautaciones razonables, pero en ninguno de estos casos se dirigió al sector privado, por la oposición tradicional de la industria norteamericana de limitar su derecho al uso de los datos personales, en su propio beneficio y como herramienta comercial, pese a ello,“ la irrupción de las nuevas tecnologías y la escasa protección legislativa de la privacidad motivó la pérdida de la confianza del consumidor norteamericano y ello forzó la auto imposición empresarial, voluntaria y como táctica comercial, como normas de conductas limitativas del libre uso de los datos personales” (Muñoz, 2016). La protección de los datos personales en EEUU, en el ámbito privado, se vino confeccionando mediante la auto

[4] Szyslak (2005). *Mapa político de los estados de Estados Unidos*. Obtenido en Wikimedia Commons

regulación de los propios sectores o empresas y no como obligación impuesta por el estado, a pesar de no contar con acciones judiciales específicas. Cabe resaltar la existencia de éstas acciones para la protección de los datos personales.

El término "privacidad" aparece por primera vez en el año 1890 en el famoso artículo "El derecho a la privacidad" (LouisD.Brandeis & D.Warreny, 1890) de los autores Samuel D. Warren y Luis D. Brandeis, en el que se destaca la necesidad de proteger el derecho más general del individual y hacen un pronunciamiento respecto a los cambios que sufren las sociedades desde el punto de vista económico, político y social, que implican el reconocimiento de derechos, como el de la privacidad y la protección de información personal.

Tomando como referencia el artículo anterior, William L. Posser en 1960 establece cuatro tipos de agravios o ataques a la privacidad: intrusión en la intimidad; publicidad denigratoria y apropiación del nombre o apariencia de otro en beneficio propio.

En 1968 el Congreso de Estados Unidos amplió la protección legal contra la vigilancia electrónica. El Título III de la Ley Omnibus de Control de la Delincuencia y Seguridad de las Calles extendió el alcance de la regulación de las intervenciones telefónicas a los oficiales estatales, así como a los sujetos privados, sin embargo dicho Título III no se aplicaba a las vigilancias de carácter visual y tampoco a otras formas de comunicaciones electrónicas.

Más adelante, se confeccionó el derecho a la privacidad informativa, como la capacidad que tienen los individuos para controlar la información que de él se comunica a terceros, plasmado por primera vez en los informes de crédito justos en 1970.

A ello debe agregarse la aprobación en 1978 de la Ley de Vigilancia de Inteligencia Extranjera o "FISA" por sus siglas en inglés, que creó una regulación distinta de la vigilancia electrónica destinada a recoger información de inteligencia extranjera, reduciendo la protección contra la vigilancia electrónica prevista en la Cuarta Enmienda. A finales de la década de 1970 la Corte Suprema tomó varias decisiones reduciendo el alcance de la protección contenida en la Cuarta Enmienda.

En 1986 se promulgó la ley de Privacidad de Comunicaciones Electrónicas, que expandió el Título III de Ley Omnibus de Control de la Delincuencia y Seguridad de las Calles de 1968[5] restringiendo la intercepción de comunicaciones transmitidas y la búsqueda de comunicaciones y archivos guardados por los proveedores de servicios de comunicaciones, así como reguló los límites de los registros de llamadas.

Luego de los ataques terroristas ocurridos el 11 de septiembre de 2001, en Estados Unidos hubo un fuerte impulso político para instaurar nuevas medidas de vigilancia y nuevos poderes de las fuerzas del orden. Con este propósito el Congreso Promulgó el "Uniendo y fortaleciendo a América proporcionando las herramientas apropiadas requeridas para interceptar y obstruir la ley del terrorismo"[6], que llevó a cabo profundos cambios en la ECPA y la FISA, entre otras normas. Posteriormente, en 2004 el Congreso promulgó la "Ley de Reforma de la Inteligencia y Prevención del Terrorismo" para facilitar la comunicación de información entre las agencias federales.

[5] Estatuto creado para regular la vigilancia electrónica para investigaciones criminales en el ámbito de Estados Unidos- a nuevos medios de comunicación, prestando una especial atención al ámbito de los ordenadores

[6] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (en adelante "USA PATRIOT Act")

I. DATOS PERSONALES: UN BIEN COMERCIALIZABLE

Nos encontramos inmersos en una sociedad revolucionada por la tecnología de la información en la que los datos personales han sido sometidos a nuevas reglas de mercado, oferta y demanda, convirtiéndose en un bien de consumo para el desarrollo del trabajo de empresarios, políticos, comerciantes y ciudadanos del común, quienes en su esfera más interna los utilizan en tiempos de ocio, consumiendo la información y transformando los datos en materia prima y el conocimiento que se deriva de ellos en productos. (Rodriguez & Julio)

Los datos personales en los nuevos modelos de negocio son utilizados para segmentar, personalizar ofertas, servicios y productos e influir en los clientes según sus necesidades. Gracias a la información derivada de los datos personales se puede conocer los gustos y preferencias de un público objetivo, manejar las estrategias de ventas, aumentar utilidades y orientar la producción a las necesidades de consumo.

Otra actividad empresarial en la cual el dato es un insumo importante es el marketing directo, esta actividad busca atraer nuevos clientes mediante el correo electrónico o mensajes de texto ofreciendo productos o servicios vinculados a las necesidades de consumo del momento.

Los gobiernos, gracias a la recolección y tratamiento de los datos personales, pueden evaluar campañas, estudios y estadísticas, no obstante, en algunos casos sus agentes o el mismo gobierno dispone sin control los datos personales, acarreando graves riesgos para los titulares y problemáticas sociales como la persecución, discriminación y exclusión.

Las entidades financieras también utilizan los datos con el propósito de conocer la solvencia real de sus clientes antes de proporcionarles cualquier tipo de crédito. (Ferrero & Schutz, 2013)

La era digital (Rubio, 2015)[7] ha facilitado la recolección, almacenamiento y transmisión de datos, haciendo que esta sea casi instantánea, permitiendo que los datos no solamente sean almacenados sino que además sigan circulando, en la mayoría de los casos, sin que el titular de los datos tenga conocimiento de quien tiene acceso a estos y quien los pone nuevamente en circulación.

La era digital y las nuevas tecnologías traen consigo ventajas para acceder a la información, haciendo que esta sea rápida y eficaz. Enviar, almacenar e interactuar con los datos personales de otras personas, en tiempo real y a nivel global, ha facilitado la interconexión entre los individuos a nivel mundial, sin embargo, esto afecta constantemente los derechos de las personas involucradas y las convierte en víctimas de las redes de tráfico de datos personales. (Franco, 2000)

La evolución de la tecnología ha logrado que cada día surjan nuevas formas de captar información, tal como los antecedentes laborales, transacciones, lugares visitados y muchos más datos sin que las personas se den cuenta. La información que se deriva de esto, no solamente es utilizada como insumo, sino que estas modernas y eficientes tecnologías permiten incluso que los datos sean circulados en cantidades ilimitadas con fines comerciales sin ningún control. (Ferrero & Schutz, 2013) Por eso los datos son una "mercancía" cotizada

[7] "(…) se manifiesta a través de un verdadera revolución tecnológica (Internet, ordenadores, dispositivos y herramientas TIC, foros, chats, blogs, medios de comunicación, etc.) que está transformando de manera clara y profunda los hábitos, el lenguaje, la vida y las costumbres de muchas personas para crear una nueva cultura.

en el mercado, cada día aumenta la solicitud de datos para brindar mejores servicio, más personalizado y acorde a intereses particulares, llevando a la realidad de desprotección donde "los titulares están lejos de llegar siquiera a imaginar el valor de sus datos, la multiplicidad de modos en que han sido manipulados, ni quienes tienen o han tenido acceso a ellos, los fines o intenciones". (Ferrero & Schutz, 2013)

De lo expuesto, se puede afirmar entonces que los datos personales se han convertido en un bien permanentemente comercializado a nivel internacional y en un insumo de los sistemas de información privados y gubernamentales, caracterizados por: i) Nutrirse de los datos personales, ii) Ofrecer múltiples posibilidades para "tratar" la información en poco tiempo y de manera imperceptible para los titulares, iii) No son absolutamente seguros, iv) Evolucionan rápidamente, y v) Traspasan las fronteras físicas, acelerando la circulación y la recolección internacional de la información. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

La normatividad en tratamiento de datos personales permite al titular identificar quien trata sus datos ya que sobre este derivan unas obligaciones y reglas para el tratamiento de los mismos, en todas y cada una de sus etapas quien trata los datos es el responsable y/o encargado de las bases de datos.

El Responsable del tratamiento de los datos personales es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. El encargado del tratamiento será aquella persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento, ambos deberán no solo realizar

sus funciones de tratamiento de manera leal, lícita y ética, de modo que no ponga en peligro los derechos fundamentales de las personas; sino también, adoptar medidas tecnológicas, administrativas, físicas y humanas tendientes a controlar el acceso no autorizado a la información y evitar su manipulación, alteración o destrucción. En síntesis, la implementación de regulaciones sobre tratamiento de datos personales. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

Los datos personales son susceptibles de ser controvertidos, y al integrarse entre sí, permiten identificar a la persona denominada titular y en principio propietario de los datos, que se encuentra ligado a las facultades de disponer, controlar y rectificar los datos. Tanto la jurisprudencia como la ley han reconocido la propiedad de los datos al sujeto como titular, otorgándole facultades para limitar la divulgación, publicación o cesión a las administradoras de la información, sin embargo, no es tajante afirmar que su uso pueda estar bajo su control.

La información contenida en los datos personales es clasificada a partir de un criterio cualitativo en función de su publicidad y facilidad de acceso, de acuerdo con las restricciones impuestas por el legislador, de la siguiente manera: Información pública (Sentencia C - 1011 , 2008)[8] o de dominio público, información semi – privada (Sentencia C - 1011 , 2008)[9]

[8] "(…) Aquella que puede ser obtenida sin reserva alguna, entre ella los documentos públicos, habida cuenta el mandato previsto en el artículo 74 C.P."

[9] "(…) Hace referencia a aquella de carácter personal o impersonal que no está contemplada en la categoría anterior y que para su acceso o conocimiento se requiere un grado mínimo de limitación. En ese sentido, la misma solo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales."

información privada (Sentencia C - 1011 , 2008)[10] e información reservada (Sentencia C - 1011 , 2008)[11] o secreta. (Sentencia T - 729 , 2002) (Sentencia C - 1011 , 2008)

La corte constitucional en sentencia T – 729 de 2002, no solo advirtió que los datos son el objeto de protección del derecho de Habeas Data, sino que estos deben cumplir con unos elementos: i) Referirse a aspectos exclusivos y propios de una persona natural, ii) Permitir identificar a la persona, en mayor o menor medida, ya sea por los datos o por la relación de estos con otros; iii) Su propiedad reside exclusivamente en el titular del mismo, sin alterarse en ningún momento, con la forma de obtención por parte del tercero, licita o ilícita y iv) Su tratamiento se encuentre sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación. (Sentencia T - 729 , 2002)

Por otro lado, cuando hacemos referencia a los administradores, estamos hablando de los responsables y/o encargados del tratamiento de los datos fuera de Colombia, llamados a cumplir con los principios establecidos y desarrollados por la jurisprudencia y la ley, que recoge en gran medida, la tendencia internacional a establecer principios de administración de los derechos personales que sirvan como sustento para la protección de los derechos fundamentales del titular, en especial la intimidad y el Habeas Data.

Los principios que la jurisprudencia ha desarrollado para que vayan de la mano con el tratamiento de los datos personales en pro de la protección de los titulares (Sentencia T - 729

[10] "(…) Puede tener contenidos personales o no y por encontrarse en un ámbito puramente privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Como ejemplos, se exponen los libros de los comerciantes, los documentos privados, las historias clínicas, los datos obtenidos en razón de la inspección a un domicilio o aquellos que se obtienen con posterioridad a la práctica de pruebas en procesos penales sujetos a reserva."

[11] "por tener carácter exclusivamente personal y por su estrecha relación con los derechos fundamentales del titular -dignidad, intimidad y libertad-, se encuentra reservada a su órbita y no puede ser obtenida ni ofrecida ni siquiera por autoridad judicial en el cumplimiento de sus funciones."

, 2002) son: el principio de libertad (Sentencia T - 729 , 2002)[12], necesidad (Sentencia T - 729 , 2002)[13], integridad, incorporación, finalidad[14], utilidad, circulación restringida[15] e individualidad; los desarrollados por la ley (Ley Estatutaria 1581 , 2012): principio de legalidad en materia de tratamiento de datos personales[16], de finalidad[17] libertad[18], de veracidad o calidad[19], de transparencia[20], de acceso y circulación restringida[21], de seguridad[22] y de confidencialidad. (Ley Estatutaria 1581 , 2012)[23]

[12] "Los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular. Se encuentra prohibido el manejo y divulgación de dichos datos, sin la previa autorización del titular o de sus representantes."

[13] "Los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos. En ese sentido, se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos a la que pertenecen o pretenden hacerlo"

[14] "La Corte ha manifestado que el suministro de datos personales debe realizarse en un contexto más o menos delimitado, es decir, que "la referida información [debe destinarse] a realizar los fines exclusivos para los cuales fue entregada por el titular, en relación con el objeto de la base de datos y con el contexto en el cual estos son suministrados". Por lo tanto, según este principio "tanto el acopio, el procesamiento y la divulgación de los datos personales, debe obedecer a una finalidad constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista."

[15] "La divulgación y circulación de la información est[én] sometid[as] a los límites específicos determinados por el objeto de la base de datos, por la autorización del titular y por el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales".

[16] "El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen"

[17] "El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular"

[18] "El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento"

[19] "La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error"

[20] "En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan"

[21] "El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;
Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley")

[22] "La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento")

[23] "Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."

II. PROTECCIÓN DE DATOS PERSONALES, MODELOS DE REGULACIÓN Y SISTEMAS DE PROTECCIÓN

Partiendo de los estándares internacionales en materia de tratamiento de datos personales, se han identificado dos modelos de regulación que han sido la referencia para los demás, un modelo centralizado y un modelo sectorial.

El modelo centralizado implementado en la Unión Europea, parte de una categoría general de datos personales y de la idea de que cualquier tratamiento de ellos es considerado por sí mismo potencialmente problemático, por la cual esta debe sujetarse a unos principios y garantías mínimos comunes, susceptibles de complementar con regulaciones especiales, según el tipo de datos y los intereses involucrados, pero de ninguna manera supone una derogación de los estándares de protección generales que son aplicables tanto al sector público como al privado.

Este modelo goza de una entidad central, autónoma e independiente encargada de supervisar la instrumentación, cumplimiento normativo y ejecución de los estándares generales de protección, cuenta además con facultades para autorizar o prohibir las transferencias de datos internacionales atendiendo a la equivalencia de la protección que ofrece el país de destino.

En contraste, encontramos el modelo sectorial implementado en EE.UU, este no parte de una categoría común de datos personales y por ello no se considera que todos estos deban estar sometidos a la misma regulación mínima. Bajo este modelo se adoptan regulaciones especiales y diferentes para cada tipo de dato personal, dependiendo de su relación con la

intimidad o privacidad como se denomina en el sistema anglosajón y con la protección de intereses superiores como la seguridad y la defensa nacional.

La regulación sectorial se basa en la ponderación de intereses que dan lugar a reglas diferenciadas, según el tipo de datos que se tratan se otorgan diferentes poderes de intervención a las autoridades.

En este modelo, la verificación del cumplimiento de las reglas también es asignada a autoridades sectoriales, que son dotadas de distintos poderes de vigilancia y control, según el nivel de intervención previsto por el legislador.

Aunque estos han sido los modelos internacionalmente reconocido hay un tercer modelo denominado híbrido, el cual países como Colombia han optado implementar. Este modelo utiliza como instrumentos tanto la regulación como la autorregulación, es decir, la implementación de normas constitucionales, generales y sectoriales junto con contratos y normas corporativas vinculantes. (Sentencia C - 748, 2011)

En el 2008 se estableció la ley 1266 de 2008, objeto de la sentencia C – 1011 de 2008, en esta se regulan los principios generales aplicables a todas las categorías de los datos personales y se establecen estándares básicos de protección para el dato financiero y comercial, destinado a calcular el nivel de riesgo crediticio de las personas.

En el 2015, con la ley 1581 de 2012, se buscó llenar el vacío de estándares mínimos de protección de todos los datos personales, dando paso al sistema híbrido del que hablamos, en el que confluyen tanto las leyes que regulan los principios generales como otras regulaciones

sectoriales, que deben leerse en concordancia con la ley general, pero que introduce reglas específicas que atienden a la complejidad del tratamiento de cada tipo de dato.

La Unión Europea con la promulgación del convenio N° 108 del 28 de agosto de 1981 fue uno de los primeros en adoptar en su legislación interna los principios mínimos de protección ante las grandes bases de información que podían poner en riesgo los derechos de los ciudadanos.

Posteriormente se adoptaron otros instrumentos internacionales como la Resolución 45/95 del 14 de diciembre de 1990 y la Directiva 95/46/CE, el primero por el Consejo de la Unión de la Organización de las Naciones Unidas y la segunda por el Parlamente Europeo.

Finalmente, fue adoptado un catálogo de 15 directrices, diseñado por la Organización de los Estados Americanos, en el cual se definió "la base de la legislación sobre protección de datos en todo el mundo y que podrían servir de base para un instrumento internacional o una legislación modelo sobre protección de datos".

En un mundo globalizado y cambiante como el de hoy, la cooperación entre estados se convirtió en algo habitual pero al mismo tiempo más complejo gracias a sus diferencias sociales, culturales, económicas y legales, razón por la cual, deciden celebrar acuerdos y tratados internacionales como medida para salvaguardar estas diferencias.

En materia de regulación de tratamiento de datos personales, pese a los intentos en busca de un consenso internacional, aun no existe unanimidad, de ahí que coexistan diferentes enfoques y modelos de protección no excluyentes entre sí, que buscan proteger los datos desde su recolección hasta el momento en que son puestos en circulación. (Muñoz, 2016)

A nivel internacional se han identificado al menos cinco alternativas de regulación, entre ellas, disposiciones constitucionales, leyes generales, leyes sectoriales, la contratación y la autorregulación. Cada país, en consonancia con el principio de jurisdicción, como manifestación de la soberanía, definirá desde donde abordar la regulación en la protección de los datos personales, muchos de ellos, como en el caso Colombiano, optan por una mixtura complementaria con el fin de garantizar un nivel mínimo de protección. (Luque, 2002)

Atendiendo a estas alternativas de regulación, el profesor Remolina Angarita, hace gran énfasis en la distinción entre los modelos de regulación y los sistemas de protección de datos personales. Los modelos de regulación se refieren a la forma de reglamentar los deberes de los responsables del tratamiento de datos y los derechos de los sujetos como titulares de los datos. Los sistemas van más allá, estableciendo además, mecanismos eficientes para el cumplimiento de esos derechos y deberes.

En algunos casos, se puede observar una fusión tanto de sistemas como de modelos; donde se incluyen en un solo texto derechos, obligaciones y mecanismos de protección y herramientas e instituciones para obligar a los responsables a cumplir con sus deberes so pena de sanciones económicas.

Los gobernantes junto con el ente regulador de cada país son quienes definen si adoptar uno u otro modelo, esto dependerá de la voluntad política y el grado de injerencia que tengan las empresas, teniendo en cuenta que los datos son el objeto de muchos negocios y estas regulaciones pueden llegar a afectar algunas industrias.

Como se ha evidenciado, Estados Unidos y Europa tienen grandes diferencias tanto normativas como ideológicas. Europa confía en el papel del estado, mientras que Estados Unidos confía en el individuo, buscando cada vez más limitar al estado. Estas diferencias hacen que en ocasiones se vean obligados a trabajar de forma conjunta para el beneficio mutuo. (NAÏR, 2013)

Frente a la normatividad de protección de datos, las diferencias entre Europa y Estados Unidos saltan a simple vista: Europa tiene una concepción de protección de datos paternalista[24], con fundamento en la máxima: "El ciudadano es el propietario de sus propios datos"; en EEUU ocurre lo contrario, su confianza está en el mercado, es decir, un enfoque liberal donde el mercado se autorregula.

La regulación de datos personales en Europa, está conformada por normas generales y sectoriales, armonizada a la existencia de una autoridad de control encargada de hacer cumplir la regulación de la norma. Desde el Parlamento Europeo se sintetizaron términos fundamentales que deben tenerse en cuenta para que un sistema de protección de datos personales este completo. i) Establecer los derechos de las personas cuyos datos se tratan y las obligaciones de quienes tratan dichos datos, ii) sanciones apropiadas para los infractores y iii) un organismo supervisor independiente. (Rodríguez, 1998.)

Lo más importante de este sistema es la protección de datos como un derecho fundamental con un enfoque preventivo, buscando evitar que se vulneren los derechos, esta protección no solo cobija a todos los ciudadanos en la UE, sino a todos en general.

[24] "Tendencia a aplicar las formas de autoridad y protección propias del padre en la familia tradicional a relaciones sociales de otro tipo; políticas, laborales, etc." Diccionario de la Real Academia Española.

La regulación en Estados Unidos, por el contrario, tiene como fundamento una mezcla de legislación, reglamentación y autorregulación. No considera la protección de datos como un derecho fundamental, sino como un derecho del consumidor, considerando innecesario la existencia de una autoridad de control especializada en el tratamiento de datos personales sin perjuicio de otras formas de control. (Lusky, 1972)

Este sistema, prefiere la autorregulación y la promulgación de varias normas sectoriales, en lugar de disposiciones generales. Es decir, no busca prevenir sino mejor resolver el conflicto. Estos conflictos son resueltos en las cortes, compensando a posteriori cuando sea necesario. Este sistema está encaminado a la protección únicamente de los ciudadanos americanos, sin embargo, para aquellas empresas Estadounidenses que quieran trabajar en suelo Europeo, se ha implementado un mecanismo llamado “puerto seguro” y por ende deberán cumplir con la normatividad Europea, permitiendo evidenciar una aproximación entre estas legislaciones. (Gonzalez, 2007)

III. COMERCIO INTERNACIONAL Y LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

La transferencia internacional de datos personales, como una de las actividades que demanda la globalización y los fenómenos de integración económica y social, que circula con mayor facilidad gracias a la era digital y a la evolución de la tecnología, es entendida como la importación o exportación de información de un país a otro, lo que supone entonces, que los datos encontrados en un país sean trasladados o enviados a otro. (Franco, 2000)

Las transferencias de los datos pueden darse de varias formas, i) entre un responsable del tratamiento del país de origen y un responsable del tratamiento del país receptor; ii) entre un encargado del país de origen y un encargado del país receptor iii) entre un encargado del país de origen y un subencargado del país receptor. En el primer caso se produce una pérdida de competencia de la ley del país de origen, a no ser que el responsable del tratamiento que actúa como importador de los datos le sea aplicable la legislación del país de origen en aplicación de normas de derecho internacional público o utilice en el tratamiento medios situados en territorio del país de origen, salvo que estos se utilicen únicamente con fines de tránsito.

Cuando la transferencia se efectúa a un encargado del tratamiento que se encuentra fuera del país de origen, no se produce esta pérdida de competencia por que el responsable del tratamiento que actúa como exportador de los datos en un establecimiento situado en el territorio de origen es quien realmente posee el control y dominio sobre los datos, decidiendo sobre su finalidad, contenido y uso. El encargado quien actúa como importador y se encuentra fuera del país de origen permanece sometido a la ley del país de origen.

La transferencia entre un encargado del tratamiento que actúa como exportador de los datos, establecido en el país de origen y un subencargado del tratamiento que actúa como importador de los datos y que se halla ubicado en un país tercero que no garantiza un nivel adecuado de protección, dado que el encargado exportador no puede decidir de forma autónoma sobre la finalidad de los datos, se requiere la existencia de un contrato marco entre este y el responsable del tratamiento en el que autorice la subcontratación y la transferencia de los datos. (Muñoz, 2016)

Esta circulación constante de los datos exige una normatividad de carácter global, cuyo diseño se ha convertido en un desafío regulador, fundamentalmente porque la protección de las transferencias internacionales de datos implica desfigurar los derechos humanos y las libertades fundamentales con los intereses del comercio internacional.

La utilidad y el valor de los datos personales dependen, en muchos casos, de la posibilidad de circulación. Aun cuando esta circulación no es libre y para que sea legítima, dependerá única y exclusivamente de casos específicos que se encuentran regulados, en algunas circunstancias es estrictamente necesaria dicha circulación para el cumplimiento de unas finalidades.

Desde 1970, se ha evidenciado la necesidad de proteger los datos personales, sin impedir su tratamiento, pero evitando lesionar los derechos de las personas. Ante esta evidente necesidad de circular internacionalmente los datos personales, han surgido reglas que deben ser tenidas en cuenta con miras a que los esfuerzos internos de protección no se desvanezcan cuando estos son objeto de transferencia internacional.

En Colombia, el desarrollo jurídico sobre la circulación internacional de los datos personales aun es deficiente. En 2008 con la ley estatutaria 1266 del 31 de diciembre de 2008, se hizo la primera referencia en el literal f) del Art. 5 de forma escueta. Luego, mediante la sentencia C – 1011 del 16 de octubre de 2008 la Corte Constitucional se refirió a esta, precisando algunos aspectos que deben tenerse en cuenta en el proceso de exportación de información personal contenida en bases de datos o ficheros que se encuentran en Colombia.

Pero solo hasta el 2009, con la ley 1273 del 5 de enero de 2009 se tipificó como delito la "Violación de datos personales", sancionando penalmente a todo aquel que sin estar facultado "ofrezca, venda, intercambie y/o envíe" datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Más adelante, con la Sentencia C – 748 de 2011 y en el Art. 26 de la ley estatutaria 1581 de 2012 de protección de datos personales, se deduce una prohibición de transferencia internacional a cualquier tipo de país que no proporcione niveles adecuados de protección de datos, sin embargo en esta misma se establece un conjunto de excepciones a la regla, permitiendo la transferencia de datos a países que pueden no tener un nivel adecuado de protección y por tanto permitiendo la transferencia en aquellos casos en los que el titular de la información ha otorgado su autorización expresa e inequívoca para la transferencia.

En esta misma sentencia, la Corte Constitucional hizo revisión de la constitucionalidad de la ley 1581 de 2012, manifestando no percibir inconvenientes, puesto que para su procedencia se prescribe que debe haber una autorización expresa e inequívoca del titular del dato y en desarrollo del principio de la libre voluntad del titular de autorizar la circulación de la

información, es claro que se permite la transferencia a un país que no brinda estándares de protección adecuada, bajo la responsabilidad de su titular.

En el 2013, con el decreto 1377 de 2013, se establece que la transferencia internacional de datos tenga lugar cuando los datos efectivamente salgan fuera del territorio colombiano. "La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país"[25]

En el ámbito internacional, las organizaciones, han establecido diversos medios para transferir datos de un país a otro en los que se debe verificar que el país importador garantice un nivel "Adecuado" de protección de los datos personales, esto con el fin de que no se afecte la protección de los interesados por el tratamiento de sus datos personales.

Cuando se habla de un "Nivel adecuado" se refiere a que el Estado importador tenga un grado de protección superior, igual, similar o equivalente al del Estado exportador, con la finalidad de evitar que con ocasión de una operación de exportación de los datos personales se disminuya el nivel de protección que se garantiza al titular del dato personal en el país exportador.

Europa es considerada pionera en establecer estándares de protección que permitan la calificación de equivalente a la protección del estado importador para la transferencia internacional cuando se transfieren a terceros países. En síntesis, que goza de un "Nivel adecuado" de protección.

[25] Art. 3, Decreto 1377 de 2013

Como lo anota el profesor Remolina Angarita, dicho nivel se refiere a que el estado importador tenga un grado de protección superior, igual, similar o equivalente al del estado exportador, dándole aplicación al principio de continuidad en la protección de datos; por lo anterior en el marco de la comisión Europea se adoptaron dos documentos de importancia: "Las primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación" y, "Transferencias de datos personales a terceros países: Aplicación de los Artículos 25 y 26 de la Directiva sobre protección de datos de la UE". (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

Teniendo en cuenta que los países no tienen un régimen de protección de datos uniforme, algunas autoridades u organizaciones internacionales, al igual que en Europa, establecieron unos principios comunes que les permitieran determinar si las normas de un país específico brindan un nivel adecuado de protección.

El Parlamento Europeo en la Directiva 95/46/CE, El Convenio 108 de 1981, Las Directrices de la Organización para la Cooperación y el Desarrollo Económico OCDE de 1980 y los Principios de la ONU de 1990, han establecido que dichos principios mínimos deben contemplar la limitación de la finalidad, la calidad de los datos y proporcionalidad, la transparencia, la seguridad, el acceso, rectificación y oposición. Deberá restringir las transferencias sucesivas a otros países y las disposiciones sectoriales o adicionales para el tratamiento de datos de tipo especial donde se incluyen, datos sensibles, mercadeo directo y decisión individual automatizada.

Esta práctica, es de continuo crecimiento, lo que hace que cada vez sean mayores las cantidades de datos que se transfieren a través de países y continentes a medida que se incrementan las relaciones sociales, económicas, los usuarios de internet y la inmersión masiva de tecnologías de información y comunicación en el mundo.[26]

Asia Pacific Economic Cooperation (APEC) es un foro multilateral de negociación en temas relativos al intercambio comercial, coordinación y cooperación entre las economías de los países que la integran, dirigido a promover y facilitar el comercio, las inversiones, la cooperación económica y la técnica entre los mismos.[27]

La APEC fue creada en 1989 en la que se incluyen países como Australia, Canadá, Corea, Chile, Estados Unidos de América, Filipinas, Indonesia, Japón, México, Nueva Zelandia, Perú, Rusia y Vietnam. Esta organización implementó la Privacy Framework, documento marco para la regulación del tratamiento de la información personal adoptado por las economías que la integran.[28] En dicho documento se buscaba establecer un estándar de protección que no impidiera el comercio internacional entre los países miembros, para el año 2004 aprobaron un marco que tenía como finalidad el fortalecimiento de la protección de la privacidad y permitir los intercambios de información, no obstante, estos no dejan de ser voluntarios, recíprocos y multilaterales, lo que no compone para sus miembros una obligatoriedad de cumplimiento.

[26] Recomendación del consejo de la OCDE relativa a las directrices que rigen la protección de la intimidad y la circulación transfronteriza de datos de carácter personal, aprobada el 23 de septiembre de 1980.
[27] Organization for Economic Co – operation and Development, Declaration on Transborder Data Flows, adopted by the Governments of OECD Menber Countries on 11 April 1985 – C (85) 139
[28] Organization for Economic Co – operation and Development, Declaration on Transborder Data Flows, adopted by the Governments of OECD Menber Countries on 8 October 1998 – C(98)177

Aunque la Privacy Framework fue inspirada en las directrices de 1980 de la OCDE, en relación con la recolección de información personal que recogen las entidades privadas y públicas, esta tiene una aplicación mucho más flexible, teniendo en cuenta sus diferencias culturales, económicas y legales. Adicional a esto, a diferencia de la OCDE, esta mira con recelo la intervención de una autoridad pública que vigile y controle el tratamiento de los datos personales, porque podría entorpecer el comercio entre los países. (Valbuena)

La UE y EE.UU, como se ha podido evidenciar, tienen un enfoque diferente para la regulación de la privacidad y la transferencia de los datos personales, sin embargo, desde 1999 se elaboró un marco de "puerto seguro" con el fin de salvar estas diferencias de enfoque y proporcionar un medio entre estos, subsanando la Directiva 95/46/CE, donde se prohíbe la transferencia de datos personales a países no pertenecientes a la Unión Europea que no cumplen con los estándares adecuados de protección de los datos personales. (Muñoz, 2016)

El programa de puerto seguro se compone de siete principios. Las organizaciones que decidan participar en este deben cumplir y declarar públicamente que llevan a cabo los principios del programa y deben ratificar su auto certificación cada año ante el departamento de comercio de Estados Unidos.[29]

El 6 de Octubre de 2015, en sentencia del Tribunal De Justicia de la Unión Europea, se anuló la decisión 2000/520/CE y consideró que los principios de Puerto seguro realmente no

[29] Description of the safe Harbor Framework Although the respective sets of safe Harbor Privacy Principles, frequently asked questions and answers (FAQs), and enforcement statements of the two Safe Harbor Franmeworks are similar, they differ in a number of ways. Understanding the safe Harbor Frameworks requires familiarity with all the relevant documentos. http://export.gov/safeharbor/ue/index.asp

garantizaban un nivel adecuado de protección de los datos personales transferidos desde la UE a EE.UU.

En el 2016, la UE y EE.UU nuevamente anunciaron su voluntad de entablar un nuevo marco regulador de las transferencias internacionales de datos, como sucesor de la declaración de puerto seguro que fue invalidada por la UE. En este nuevo acuerdo EE.UU se compromete por primera vez a establecer garantías, limitaciones y mecanismos de supervisión al acceso de datos personales transferidos desde la UE, a las autoridades públicas estadounidenses. EE.UU, ha descartado la realización de actividades de vigilancia masiva indiscriminada de los datos personales transferidos y se propone controlar este nuevo marco regulador mediante una revisión conjunta anual efectuada por la comisión y el Departamento de Comercio de los EE.UU, asistiendo como invitados expertos en inteligencia de los EE.UU y autoridades Europeas de protección de datos.

Otro de los cambios de este nuevo marco regulador es la imposición de plazos a las empresas para responder las quejas efectuadas por los particulares, eliminación de costos para los procesos de reclamación y acceso a los mecanismos de resolución alternativa de conflictos. Las autoridades Europeas podrán derivan también las quejas de los particulares al departamento de comercio y a la comisión federal de comercio estadounidense, en la que se dará solución por medio de un nuevo defensor especializado en la materia. (Muñoz, 2016)

A pesar de todos los cambios de este nuevo marco regulatorio, EE.UU. no cumple el requerimiento principal de la UE, según el cual la protección adecuada de los datos debe otorgarla el ordenamiento jurídico en razón de su legislación interna y compromisos internacionales. (Luque, 2002)

IV. CONCEPTUALIZANDO EL "NIVEL ADECUADO DE PROTECCIÓN DE DATOS" Y "PUERTO SEGURO"

En consideración a lo mencionado en el capítulo anterior y haciendo referencia al tema que compete desarrollar en este capítulo, uno de los requisitos exigidos para poder realizar la transferencia es que el país receptor cuente con un "*Nivel adecuado de protección de datos*" o se haya declarado públicamente parte del programa de "*puerto seguro*".

"Nivel Adecuado"

La expresión *"Adecuado*" como lo indica el profesor Remolina Angarita, hace referencia a que el Estado importador tenga un grado de protección superior, igual, similar o equivalente al Estado exportador en protección de datos, en aplicación al principio de continuidad. (Angarita, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar Europeo? , 2010)

Algunas entidades internacionales, han desarrollado pautas que permiten evidenciar si el país importador garantiza un nivel "*Adecuado*" de protección de datos personales. Pablo Palazzi, en "*Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado",* expone que estas reglas buscan evitar la creación de paraísos informáticos; jurisdicciones donde la carencia de leyes de protección de datos, las transforme en sitios atractivos para realizar tratamientos de datos personales que puedan ser violatorios de otras leyes de privacidad. (Palazzi, 2003)

Lo que supone, que el nivel de protección del país exportador se garantice en el país importador, y por consecuencia no afecte la protección de los interesados por lo que respecta al tratamiento de sus datos personales.

Algunas de estas pautas desarrolladas por organizaciones internacionales son:

1.1. El consejo de la Organización para la Cooperación y el desarrollo Económico (OECD) en 1980

La OECD, con miras a fomentar la libre circulación de la información y evitar la creación de obstáculos injustificados al desarrollo de las relaciones económicas y sociales entre los países miembros, que podrían ocasionar graves trastornos a los sectores económicos, aprobó una serie de recomendaciones. Dichas recomendaciones no son un instrumento jurídico vinculante o de obligatorio cumplimiento, sino más bien unas directrices para que sus miembros tengan en cuenta a la hora de establecer sus regulaciones internas, procurando eliminar las barreras injustificadas a la circulación transfronteriza de datos personales.

La OECD, hizo énfasis para que todos los países miembros adopten todas las medidas razonables y oportunas que permitan garantizar la circulación transfronteriza, ininterrumpida y segura de los datos, así como la implementación de limitaciones para la transferencia de algunas clases de datos que pueden lesionar la intimidad y las libertades individuales.

Como se evidencia, para la OECD la regla general es la libre circulación entre sus miembros, salvo i) Que el país de destino de la información "*no haya observado sustancialmente estas directrices*" o ii) Que *"La reexportación de tales datos soslayase su legislación nacional sobre la intimidad*".

De manera que el cumplimiento de las directrices por parte de un país destinatario de la circulación transfronteriza de datos, es el factor determinante para considerar que este garantiza un nivel de protección equivalente. No obstante, estas solo prevén que dicha circulación sea entre países miembros, es decir, que operan en un escenario cerrado; de manera que para aquellos casos en los que la transferencia se hace a un país no miembro, la OECD no fija pautas, lo que permite concluir que la regla que rige la transferencia a países no miembros, será la de no enviar datos a menos que garanticen un "Nivel de protección equivalente" al que se obtiene con las recomendaciones de la OECD.

En el 2013, se hacen varias precisiones a las Directrices de 1980, donde se establece que el responsable del tratamiento seguirá siendo responsable de los datos personales bajo su control sin tener en cuenta la ubicación de estos. Se recalca además que los flujos transfronterizos no deben restringirse entre los países de la OECD ni a terceros países fuera de éste, cuando i) Se observen sustancialmente las directrices, o ii) Se cuente con suficientes salvaguardias, incluyendo los mecanismos de aplicación efectiva y medidas apropiadas que utiliza el responsable para garantizar un nivel de protección consistente con esas directrices. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

1.2. La Organización de las Naciones Unidas, en la resolución 45/95 del 14 de diciembre de 1990

La ONU se refiere a un *"Nivel adecuado de protección de datos*", cuando el país importador ofrece garantías comparables de protección a las ofrecidas por el país exportador. Si bien no consagra qué se entiende por "*Garantías comparables*" ni establece los criterios para

establecer en qué casos se está frente a garantías "*comparables*", esta adopta unos principios rectores, dentro de los cuales se encuentra el denominado flujo de datos a través de las fronteras, en el que se considera que dos o más países involucrados en el flujo de datos a través de sus fronteras, ofrezcan legislativamente un nivel comparable de protección y la información pueda estar libremente como dentro de su propio territorio.

A pesar de que la ONU no precisa qué se debe entender por garantías comparables, se puede inferir que el objetivo es circular los datos a territorios donde las garantías de protección sean equiparables, semejantes, similares o análogas a las del país exportador. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)r.

1.3. El consejo de Europa en el convenio 108 de 1981

El consejo estableció unas pautas para proteger a las personas respecto al tratamiento automatizado de datos de carácter personal. En lo referente al tema, habla del flujo transfronterizo de datos de carácter personal y el derecho interno, estas pautas dependen de si los datos se envían a países que hacen parte o no del convenio, de ahí que el flujo internacional de datos sea libre entre estados parte del convenio y prohibido o condicionado cuando se realiza a un estado no parte del mismo.

Cuando el país importador hace parte del convenio no existe inconveniente en que se envíen los datos y no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial el flujo transfronterizos con destino al territorio de otra parte.

Si el país importador no hace parte del convenio, será posible prohibir o condicionarse a la autorización especial el flujo internacional de los datos, con el fin de evitar que estas transmisiones tengan como resultado burlar la regulación de la parte contratante. En el 2001, mediante protocolo adicional al Convenio 108, se modificó la anterior prohibición del flujo internacional a un lenguaje permisivo, condicionado a que el Estado importador garantice un nivel adecuado de protección.

Conforme a lo anterior, se introdujo la expresión "*Nivel adecuado de protección*" y se dio la posibilidad de permitir la transferencia, aun cuando esta no se cumpla si existen otras garantías o alternativas de protección, como las cláusulas contractuales, dichas garantías deberán ser consideradas adecuadas por parte de las autoridades competentes del país exportador de los datos. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

1.4. Foro de Cooperación Económica Asia – Pacifico

Para el Foro las transferencias internacionales se basan en un sistema voluntario de certificación de buenas prácticas que son vinculantes para las organizaciones que las adoptan. En el marco de privacidad APEC de 2004, se incorporaron ciertos aspectos de las transferencias internacionales en el principio de responsabilidad, donde se establece que cuando los datos van a ser transferidos internacionalmente, el responsable tiene dos opciones: i) Tener autorización del titular de la transferencia, o ii) Actuar con la debida diligencia y tomar las medidas razonables para asegurar que las personas u organizaciones receptoras, tengan protegida la información consistentemente con los principios.

Dado que, la autorización no es obligatoria, el responsable debe velar por que la organización o empresa receptora de la autorización garantice un nivel adecuado de protección, en concordancia con los principios APEC de 2004. No obstante, el responsable deberá cumplir con las leyes del país donde se van a exportar los datos, de manera que la ley local podrá permitir la transferencia internacional cuando se utilicen mecanismos de autorregulación, como las normas corporativas vinculantes.

La operatividad de las reglas de transferencia internacional entre los países que hacen parte del APEC implica que, tanto los gobiernos como empresas u organizaciones exportadoras de datos, cumplan con unos pasos, algunos de competencia de las autoridades públicas y otros de quien desee transferir desde un país APEC. Las autoridades gubernamentales deben aplicar para formar parte del Cross Border Privacy Enforment Arrangement (CPEA), con miras a crear un marco de cooperación transfronteriza en la aplicación de las leyes sobre protección de datos, en las eventuales investigaciones sobre infracciones a las normas sobre dicho tema.

Simultáneamente, las autoridades locales competentes de cada país, deben presentar una solicitud para participar en el CBPR System. Las empresas de cada país que deseen participar en el sistema deben acreditarse ante un Accountability Agent (AA) reconocido por el APEC y serán responsables de la elaboración de políticas y prácticas de tratamiento de datos de obligatorio cumplimiento. En aquellos casos en los que se incumplan, podrá haber sanción por parte de los AA o por las autoridades de cada país.

Aquellas empresas que se encuentran acreditadas por los AA, hacen parte de un directorio de acceso público con los datos de contacto, de manera que estas queden habilitadas para

transferir datos o cuando los titulares de los datos lo estimen necesario, puedan elevar consultas, reclamos o se quejas ante las autoridades de control, si evidencian alguna irregularidad.

Este sistema no deja sin efectos las leyes nacionales ni elimina la responsabilidad de los reguladores nacionales y las autoridades de protección de datos locales, mucho menos exime a las empresas de cumplir con las normas sobre tratamiento de datos personales de cada país. La aplicación del CBPR en un país debe condicionarse a su permisibilidad o viabilidad jurídica a la luz de las normas locales. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

1.5. El parlamento Europeo y el consejo de la Unión Europea, con la directiva 95/46/CE de 1995

La UE reconoce la necesidad e importancia del flujo internacional de datos personales, de ahí que la circulación transfronteriza entre estados miembros sea libre, y por consiguiente, estos no puedan restringir ni prohibir la libre circulación de datos personales entre los estados miembros.

Cuando se trata de transferencias a estados no miembros o terceros países, se permiten, siempre y cuando se cumplan algunos requisitos establecidos en el capítulo IV Art. 25 y 26 de dicha directiva y donde se desarrollan las principales reglas aplicables sobre el particular, las transferencias a un tercer país, únicamente cuando el país garantice un nivel adecuado de protección, es decir, no se permite la transferencia de datos a terceros si estos carecen del nivel mínimo de debido tratamiento de datos personales.

Para hablar de "*Nivel adecuado de protección*" debemos remitirnos al Art. 25[30] de la Directiva 95/46/CE donde se establecen las pautas y factores para evaluar si el país de destino de la transferencia internacional cuenta con dicho nivel de protección.

Bajo las normas de la Directiva 95/46/CE no es sencillo ser catalogado como un país con nivel adecuado de protección de datos, para esto, se exige que los países expidan regulaciones apropiadas y efectúen cambios institucionales. Este trámite ante la comisión Europea, se demora alrededor de 2 años, con escasa probabilidad de que la comisión adopte resoluciones de adecuación para numerosos países a corto plazo, incluso a mediano plazo.

Ahora bien, al igual que en los casos anteriormente expuestos, existe una serie de casos excepcionales en los que se puede enviar información a países que no tengan nivel adecuado de protección, siempre que se cumplan las condiciones enunciadas en el Art. 26[31], estas coinciden con las excepciones previstas en el Art. 26 de la ley 1581 de 2012.

---

[30] Artículo 25. Principios
1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.
2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.
3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.
4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.
5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.
6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.
Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión. Directiva 95/46/CE

[31] Artículo 26. Excepciones

En lo que respecta al tratamiento de datos personales se han elaborado directrices que ayudan a realizar la evaluación de garantías o condiciones básicas para que sean viables las transferencias a países que no garantizan un nivel adecuado de protección de datos personales, algunas de estas estrategias son los contratos, las cláusulas contractuales, entre otras, reiteradas en el protocolo adicional al Convenio 108 suscrito el 8 de noviembre de 2001.

1.6. En Colombia

Solo hasta finales de 2008 se incorporaron reglas sobre transferencias internacionales de datos personales en Colombia, en el art. 5 de la ley estatutaria 1266 de 2008, *"La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los*

---

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:
a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o
b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o
c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.
2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.
3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.
En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.
Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.
4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

operadores que haga parte del banco de datos que administra, podrá ser entregada de manera verbal, escrita, o puesta a disposición de las siguientes personas y en los siguientes términos: F) (...)a otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuera un banco de datos extranjero, la entrega sin autorización del titular solo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular." (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

El literal f) mencionado en el parágrafo anterior, concede al operador y no a la Superintendencia de Industria y Comercio la facultad de establecer si un país diferente a Colombia garantiza el nivel adecuado de protección, haciéndolo problemático, sin embargo cuando se determina que el banco de datos extranjero garantiza un tratamiento adecuado a los datos personales de los colombianos no queda como responsabilidad de estas autoridades de la república, sino en cabeza de los operadores.

Por lo que se puede evidenciar que, con la disposición anterior se promociona el flujo internacional de los datos sin garantías ni control en beneficio del titular, se da un tratamiento que revela el desconocimiento de las implicaciones que conlleva el flujo internacional indebido para el país y los ciudadanos. Con la ley 1581 de 2012 se dejó sin efectos este literal.

Mediante sentencia C – 1011 de 2008, la Corte constitucional aunque avaló dicha ley, indicó que debían hacerse aclaraciones y declaratorias de inexequibilidad, haciendo dos precisiones frente a la transferencia de datos:

- Recalcó que debe existir necesariamente autorización previa y expresa del titular permitiendo transmitir sus datos, descartando la posibilidad de transferencia internacional sin el consentimiento del titular. (Sentencia C - 1011 , 2008)[32]
- Si bien le corresponde al operador verificar que el otro país otorga garantías suficientes para la protección de los derechos del titular, la Corte reglamentó que le corresponde a la superintendencia de industria y comercio y a la superfinanciera determinar los parámetros que deberá tener en cuenta este operador para la verificación, es más, que estas podrán identificar los ordenamientos jurídicos extranjeros de los cuales se puede predicar un nivel adecuado de protección.
- Para terminar, la Corte estatuyó que la administración de datos personales que venían del exterior debían regirse por las previsiones de la constitución y la ley colombiana sin importar que dicha información tenga origen extranjero, debiendo estar subordinados a las condiciones, requisitos y sanciones previstas en el ordenamiento colombiano.

Con la ley 1581 de 2012, se prohíbe como regla general la transferencia internacional de datos personales en el Art. 26, que consiste en no enviar datos a países que carezcan de niveles adecuados de protección, siguiendo los lineamientos de varios documentos

[32] "el titular debe expresar unívocamente su voluntad en el sentido de expresar si autoriza la inclusión de datos […], su uso para una finalidad específica y suficientemente identificable y si permite que los operadores puedan poner a disposición dichos datos a otros operadores, nacionales o extranjeros".

internacionales. En ésta, se habla de un nivel adecuado cuando el sistema jurídico de dicho país garantiza un grado de protección igual o mayor al que proporciona el sistema Colombiano, sin olvidar que el nivel adecuado no trata solo de comparar las normas entre los países, sino también de evaluar los mecanismos de protección con que cuenta el titular y verificar la existencia de autoridades independientes, técnicas y eficientes para la protección de datos.

Partiendo de los lineamientos adoptados por la Unión Europea, se entiende que un país cuenta con los estándares de garantía necesarios para un nivel adecuado de protección, si su legislación cuenta con unos principios que abarquen las obligaciones y derechos de las partes, de los datos, mecanismos y autoridades que efectivicen la protección de la información, lo que significa que el país al que se transfiere los datos no podrá en ningún caso proporcionar un nivel inferior al de origen.

En el caso Colombiano, para establecer que otro país cumple con un nivel adecuado, se deben tener en cuenta los estándares de la Superintendencia de Industria y Comercio, regulados por el art. 26 de la ley 1581 de 2012 y el decreto 1377 de 2013 que reglamentó parcialmente la ley. En ninguno de los casos podrá ser inferior a los que la ley exige para sus destinatarios.

Sin embargo, dicha prohibición no es tajante, la ley habla de algunos casos excepcionales:

- Si el titular ha autorizado de manera expresa e inequívoca la transferencia. Consentimiento explícito, claro e indiscutible del titular.[33]

[33] literal c) del art. 13 de la ley 1581 de 2012, Art. 26 "[…] se deja establecido que la premisa de contar con la autorización del titular de la información que es objeto de transferencia, es el presupuesto que permite la circulación de los datos consagrados en las otras excepciones previstas en el presente artículo del proyecto de ley y que será su condición para la respectiva declaratoria de constitucionalidad"

- Cuando se trate de datos de carácter médico y el envío sea necesario por motivos de salud o higiene pública. La facultad de autorizar esta transferencia no recae en el titular sino en sus familiares o representante legal.
- Con ocasión de transferencias bancarias o bursátiles siempre y cuando se cuente con el consentimiento previo, expreso e inequívoco del titular.[34]
- Cuando ello sea necesario para dar cumplimiento a tratados internacionales de los que haga parte Colombia.
- Siempre y cuando se cuente con la autorización del titular, si son necesarios para la ejecución de un contrato entre el titular y el responsable del tratamiento o para la ejecución de medidas precontractuales.
- Si son legalmente exigidos para la salvaguardia del interés publico
- Para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

El art. 21 de la ley 1581 de 2012, señala que dentro de las funciones de la Superintendencia de Industria y Comercio se encuentra el de *"Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos*" e "*Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los responsables del tratamiento y encargados del tratamiento a las disposiciones previstas en la presente ley*"

Finalmente, en marzo de 2017 se emite una circular en la que se adiciona un capítulo Tercero al Título V de la Circular Única, sobre transferencia internacional de datos personales, en el

[34] "en relación con las transferencias bancarias o bursátiles previstas en el literal C), las mismas se regirán de conformidad a lo dispuesto por la ley 1266 de 2008, la cual reglamenta el manejo de la información financiera, crediticia y comercial, pero bajo el entendido que la transferencia se hará contando con la autorización prevista y expresa del titular del dato" Sentencia C - 748 , " Control de constitucionalidad al proyecto de ley estatutaria N° 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales" (Corte Constitucional. Sala plena. (M.P. Jorge Ignacio Pretelt Chaljub) 6 de Octubre de 2011).

que establece los estándares del nivel adecuado de protección en el país receptor de la información, en los que se encuentran los siguientes:

a) Existencia de normas aplicables al tratamiento de datos personales
b) Cumplir con la normativa de principios aplicables al tratamiento de datos, entre los cuales deben estar: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
c) Establecer los derechos de los titulares
d) Establecer deberes para los Responsables y Encargados
e) Establecer medios y vías judiciales y/o administrativos para garantizar la tutela de los derechos de los titulares y exigir el cumplimiento de la ley
f) Crear una autoridad(es) publica(s) encargada(s) de la supervisión del tratamiento de datos personales, del cumplimiento de la legislación aplicable y de la protección de los derechos de los titulares.

Por último, realiza un listado de los países que hasta ahora cuentan con un nivel adecuado de protección reconocido por esta autoridad.

"Puerto Seguro"

El programa de "puerto seguro" está compuesto por siete principios contenidos en el acuerdo, todas aquellas organizaciones que han decidido hacer parte de este deben cumplir y declara públicamente que lo hacen, así también deberán cada año ratificar la auto certificación ante el departamento de comercio de Estados Unidos para garantizar los beneficios del programa y demostrar que siguen cumpliendo con los requisitos.

- Notificación: o deber de información. Todas las entidades deben informar a los interesados de las finalidades para las cuales han sido recabados sus datos y sobre la forma en que se utilizan.
- Consentimiento: Le corresponde al interesado o afectado el poder de decidir acerca de la recogida y transferencia de sus datos personales.
- Transferencia: Solo es posible la transferencia de datos cuando las entidades destinatarias están suscritas al acuerdo de puerto seguro o sean miembros de la UE.
- Acceso: Las personas deben tener acceso a su información y corregirla o eliminarla si no es exacta, a efectos de poder ejercitar los derechos ARCO.[35]
- Seguridad: Se deben adoptar medidas técnicas y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, perdida o acceso no autorizado.
- Calidad: Los datos deben ser fiables y consecuentes con el propósito para el que fueron recopilados.
- Aplicación: Concreta aplicación o ejecución, es un principio controvertido por ser ambiguo, busca que para garantizar el cumplimiento de los principios de puerto seguro, se deben articular además mecanismos independientes de resolución de conflictos y verificación de cumplimiento con potestad de sancionar. (Valbuena)

No obstante, la falta de transparencia y control en la ejecución de este régimen sumado al incumplimiento por las empresas auto certificadas a 2013, la ausencia de políticas de

[35] Derechos de acceso, rectificación, cancelación y oposición

privacidad por parte de las entidades y la existencia de alegaciones falsas de adhesión al puerto seguro por entidades que nunca habían participado en el marco de puerto seguro o entidades que se habían adherido a él pero no enviaron las renovaciones anuales de su auto certificación al departamento de comercio, no permitieron que se cumpliera realmente la función para la que se creó; la de proteger a los titulares de los datos personales que se encuentran fuera del territorio donde se están tratando, muy por el contrario estos están siendo una herramienta para la desprotección de los titulares cuando estos traspasan las fronteras del país de origen.

V. LA AUTORIZACIÓN Y OTROS INSTRUMENTOS DEL DERECHO CONTRACTUAL

La transferencia de datos a nivel internacional se da de manera legítima cuando el responsable de los datos personales del país de origen recolecta los datos del titular respetando sus derechos; solicitando de manera expresa, previa e informada su autorización, no solo para el tratamiento de datos sino también para hacer transferencias internacionales. El responsable debe comprometerse de igual forma a hacerlo solo hacia aquellos lugares donde tengan un nivel adecuado de protección o estén acogidos mediante acuerdos y se dé cumplimiento a las normas de tratamiento de datos del país de origen.

Autorización

La autorización, es por regla general, la forma de legitimación del tratamiento de datos. Esta deberá ser previa, informada y expresa, lo que significa que el titular del dato debe manifestar clara y explícitamente que sí autoriza el tratamiento de sus datos, por cualquier medio que pueda ser objeto de consulta posterior, haciendo excluyente la posibilidad de que el titular conceda su autorización de forma implícita o tácita, salvo en aquellos casos en los que la ley lo permita. (Ley Estatutaria 1581 , 2012)[36]

> *"[…] Los datos personales solo pueden ser registrados y divulgados con el consentimiento libre, previo, expreso, e informado del titular. Las únicas excepciones posibles serán las establecidas en el art. 10 de la ley 1581 de 2012. En consecuencia*

[36] Artículo 9°. Autorización del Titular. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

> *no está permitido el consentimiento tácito del titular del dato. El consentimiento que brinde la persona debe ser definido como una indicación especifica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales"* (Sentencia C - 748, 2011)[37]

El decreto 1377 de 2013 reguló uno de los modos de obtener la autorización mediante conductas inequívocas del titular que permitieran inferir de forma razonable que se está otorgando dicha autorización. (Decreto 1377 , 2013)[38] Esta deducción a partir de una conducta del titular, será válida solo cuando se deriva de forma lógica, conforme a razones sensatas, justas o prudentes que permitan llegar a la conclusión que éste autorizo la recolección de sus datos. Dicho de otra manera, cuando su forma de actuar, proceder, comportarse o reaccionar ante ciertas situaciones permite inferir que expresa su consentimiento para el tratamiento de sus datos.

El consentimiento en Colombia es de vital importancia. El tratamiento de datos personales está ligado a la protección constitucional de derechos, como el de libertad[39], lo que supone

---

[37] "Control de constitucionalidad al proyecto de ley estatutaria N° 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales" (Corte Constitucional. Sala plena. (M.P. Jorge Ignacio Pretelt Chaljub) 6 de Octubre de 2011).

[38] Artículo 7°. Modo de obtener la autorización. Para efectos de dar cumplimiento a lo dispuesto en el artículo 9° de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 del presente decreto, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca

[39] Artículo 15." Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de

entonces que el responsable del tratamiento de los datos personales debe respetar la facultad que le otorga la constitución a cada uno de los titulares, para decidir si autoriza o no a terceros para que traten su información. No obstante, hay algunos casos enunciados taxativamente por la ley y la jurisprudencia en las que se permite el tratamiento de los datos sin previa autorización. (Ley Estatutaria 1581 , 2012)[40]

En el ámbito internacional cada país u organización define las situaciones en las que la legitimación del tratamiento proviene de motivos diferentes al consentimiento, de los cuales se pueda inferir dicha autorización, sin embargo, de esta posibilidad se desprenden problemáticas radicadas en dos puntos importantes:

i) La subjetividad de interpretación de las conductas. En tanto, para algunos una acción del titular podrá ser una forma clara de consentir el tratamiento, como para otros no lo será, generando incertidumbre jurídica y desgaste en debates interpretativos.

ii) Si se concluye que el titular autorizó a través de dichas conductas, el reto es determinar los fines específicos del tratamiento legitimado por esta vía. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

---

las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar. Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley". Modificado por Acto Legislativo 2/2003.

[40] Artículo 10. Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:
a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
b) Datos de naturaleza pública;
c) Casos de urgencia médica o sanitaria;
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
e) Datos relacionados con el Registro Civil de las Personas.
Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

Por lo anterior, aun cuando se permita legitimar la autorización mediante conductas inequívocas del titular de los datos, este debe ser informado de las finalidades del tratamiento de sus datos, y solo a partir de ese momento, se podrá concluir para que fines autoriza el tratamiento mediante su comportamiento.

Este deber de información, debe ser claro y expreso sobre: a) El tratamiento y la finalidad a la cual serán sometidos los datos; b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando versen sobre sus datos sensibles o de niños, niñas y adolescentes, c) Los deberes físicos, electrónicos y telefónicos del responsable del tratamiento. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

En el ámbito internacional se reconoce el deber de informar previamente al titular, por la Directiva 95/46/CE, como un derecho derivado del principio de transparencia y establece que el responsable del tratamiento deberá comunicar a la persona de quien se recaben los datos que le conciernen, por lo menos, a) La identidad del responsable b) Los fines del tratamiento. C) Cualquier otra información.[41]

[41] Directiva 95/46/CE, sección IV. Art. 10 "información en caso de obtención de datos recabados del propio interesado. Los estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello. A) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como; i) los destinatarios o las categorías de destinatarios de los datos. ii) el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder. iii) la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado."

La Red Iberoamericana de protección de datos (2007), en los numerales 4 y 4.1, establece que el responsable deberá informar al momento de recolección de la información, los fines para los que los datos vayan a ser tratados y el modo en que podrá hacer efectivo los derechos del titular, derivado también del principio de transparencia.[42]

La Resolución de Madrid en el 2009, al igual que los anteriores, se encuentra ligado al principio de transparencia. El responsable deberá identificarse ante el titular de los datos, informar la finalidad para la que pretende tratar los datos, los destinatarios a los que pretende cederlos y el modo en el que el titular podrá ejercer sus derechos. A diferencia de las anteriores, La Resolución de Madrid habla no solo del deber de información cuando los datos son obtenidos directamente por el titular, sino también cuando estos son recogidos a través de redes de comunicaciones electrónicas, y en ambos casos, deberá cumplirse con el deber de información, ya sea informando directamente al titular o mediante la publicación de políticas de privacidad fácilmente accesibles e identificables.[43]

El Reglamento General de protección de datos del Parlamento Europeo y del Consejo en 2012, estableció el deber del responsable de informar, al menos su identidad y datos de

[42] "4. transparencia e información al interesado 4.1. el interesado del que se recaben los datos deberá ser informado al tiempo de su recogida de la identidad del responsable del tratamiento, los fines para los que los datos vayan ser tratados y el modo en que podrá hacer efectivos los derechos a los que se refieren los apartados 5 y 6 de estas directrices, así como de cualquier otra información necesaria para garantizar un tratamiento licito de los datos. […]"

[43] Resolución de Madrid de 2009, Art. 10, numerales 2, 3, 5 y 6. principio de transparencia. […]

2. La persona responsable deberá facilitar a los interesados al menos, información acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos previstos en el presente documento, así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.

3. cuando los datos de carácter personal hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitada con anterioridad […]

5. cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos especialmente a menores de edad.

6. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartad podrán satisfacer mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos"

contacto, los fines del tratamiento, el plazo de conservación de los datos, la existencia de medios de control, los destinatarios, cuando procede la transferencia y cualquier otra información necesaria para garantizar un tratamiento de datos leal, respecto del interesado.[44]

En definitiva, la autorización no garantiza por sí sola el debido tratamiento de los datos, es una obligación del responsable y/o encargado, que tiene un efecto simbólico y reivindicador de la dignidad humana y de la libertad de decidir para el titular de los datos, que le permite además reconocer la propiedad de estos, la facultad de decidir a quien, como y cuando otorgarlos y la facultad de exigir la protección de sus derechos y libertades. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

Acuerdos contractuales

[44] Reglamento General de protección de datos del Parlamento Europeo y del Consejo en 2012, "capitulo III: Derechos del interesado. Sección 2. Información y acceso a los datos. Art. 14 – información al interesado.
1. Cuando se recojan datos personales relativos a un interesado, el responsable del tratamiento le facilitara, al menos, la siguiente información: a) la identidad y los datos de contacto del responsable del tratamiento y, en su caso, del representante del responsable del tratamiento, y, en su caso, del representante del responsable del tratamiento y del delegado de protección de datos; b) los fines del tratamiento a que se destinan los datos personales, incluidas las clausulas y condiciones generales del contrato cuando el tratamiento se base en el artículo 6°, apartado 1, letra f) ; c) el plazo durante el cual se conservaran los datos personales d) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión o a oponerse al tratamiento de dichos datos personales; e) el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma; f) los destinatarios o las categorías de destinatarios de los datos personales; g) cuando proceda, la intención del responsable del tratamiento de efectuar una transferencia a una decisión de adecuación por parte de la comisión; h) cualquier otra información que resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado, habida cuenta de las circunstancias específicas en que se recojan los datos personales.
2. Cuando los datos personales se recojan del interesado, el responsable del tratamiento le comunicara, además de la información contemplada en el apartado 1, si el suministro de datos personales es obligatorio o voluntario, así como las posibles consecuencias de que no se faciliten tales datos […]
4. el responsable del tratamiento facilitara la información contemplada en los apartados 1, 2 y 3; a) en el momento en que los datos personales se obtengan del interesado […]"

La autorregulación, ha sido otra de las herramientas que algunos Estados a nivel internacional le han otorgado a los responsables y/o en cargados para cumplir con "garantías suficientes" para el tratamiento de los datos personales, cuando estos sobrepasan el ámbito territorial.

Una de ellas es el contrato de transferencia internacional de datos personales, aunque en Colombia solo está previsto el contrato para los casos de transmisión[45], es de gran importancia analizarlo desde la perspectiva internacional, su alcance y modo de aplicación.

La Unión Europea, mediante la directiva 95/46/CE, ha permitido mediante acuerdos contractuales establecer condiciones mínimas que garanticen un nivel adecuado de protección de datos personales cuando estos sean transferidos a un país no catalogado con el nivel adecuado de protección, a la luz de la regulación Europea, sin ser excluyente para los países que cuentan con un nivel adecuado de protección.

Los contratos, entonces, se han convertido en un instrumento jurídico de mayor relevancia para las empresas que requieren el flujo internacional de datos personales en su gestión. En este sentido,

> "*Las cláusulas contractuales tipo son una de las diversas posibilidades […] para la transferencia legitima de datos personales a un tercer país […]. Facilitaran enormemente a las entidades la transferencia de datos personales a terceros países mediante la incorporación de las cláusulas contractuales tipo en un contrato".*[46]

[45] En la transmisión el tratamiento sigue bajo la responsabilidad del responsable, quien entrega los datos al encargado para que realice el tratamiento por su cuenta y siguiendo sus instrucciones. Numeral 5° del art. 3° del decreto 1377 de 2013.
[46] Numeral 5° de los considerados de la Decisión 2001/497/CE. La Comisión de las comunidades Europeas. Decisión de la comisión de 15 de junio de 2001 "relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la directiva 95/46/CE.

No obstante, el contrato en sí mismo, no se convierte automáticamente en el instrumento que autorice la exportación de información personal desde Europa. Es necesaria además, la aprobación de la autoridad de control del país exportador.

Lo que supone entonces que el uso de este instrumento da luz verde al flujo internacional, pero será potestad de las autoridades competentes de cada uno de los Estados prohibir o suspender la circulación de los mismos, cuando se presenten algunos de los siguientes casos.[47]

i) La legislación del estado importador imponga desviaciones a las normas sobre protección de datos que van más allá de las restricciones necesarias en una sociedad democrática e implica un efecto negativo significativo sobre las garantías previstas en las cláusulas contractuales tipo.

ii) Cuando el importador incumpla las obligaciones fijadas en las clausulas;

iii) Cuando exista un alto grado de probabilidad de violación a las clausulas y con ello se genere un riesgo inminente de causar graves daños a los titulares de los datos;

iv) Cuando el importador no coopere con las autoridades de protección de datos y

v) Cuando el exportador de los datos no aporte los medios para hacer cumplir el contrato al importador. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

Este instrumento fue adoptado por las decisiones 2001/497/CE, 2002/16/CE, 2004/915/CE, 2010/78/CE y la resolución de la Agencia Española de Protección de Datos de Autorización

[47] Numeral 1° del art. 4° de las decisiones 2001/497/CE y 2002/16/CE; numeral 2° del art. 1° de la decisión 2004/915/CE

de transferencia internacional de datos de 16 de octubre de 2012, donde se hallan las clausulas tipo que aportan garantías necesarias de protección de los datos personales de los titulares, sin embargo, debemos hacer la siguiente salvedad: tanto las decisiones 2001/497/CE y 2004/915/CE sugieren modelos de contratos cuando la administración de los datos personales pasa de un operador a otro que se encuentra en un país diferente, mientras que la decisión 2010/78/CE y la resolución de la Agencia Española de Protección de Datos de Autorización de transferencia internacional de datos de 16 de octubre de 2012, comprende un esquema de contrato para aquellos casos en que la administración de la información está bajo responsabilidad de un operador que acude a un tercero ubicado en otro país para que se encargue del tratamiento. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

Normas corporativas vinculantes

Otra de las formas de autorregulación que se utiliza particularmente en modelos de transferencias internacionales, como el de la Agencia Española de protección de datos, son las Normas corporativas vinculantes, definida como el conjunto de normas que se aplica a una pluralidad de responsables del tratamiento que pertenecen a una misma profesión o sector industrial, cuyo contenido o profesión utilizados en las transferencias internacionales son consistentes con el debido tratamiento de datos personales, pero que no tienen sentido si solo se trata de un documento interno que no se cumple y del cual no se tiene mecanismos de auditoria y verificación. Para la Corte Constitucional,

> *"Esas normas de autorregulación en la práctica internacional son generalmente revisadas por las autoridades nacionales del protección de datos, que deben vigilar*

> *que se consagren y garanticen salvaguardias adecuadas para transferencias o categorías de transferencias de datos personales entre empresas que forman parte del mismo grupo corporativo. En consecuencia, la corte considera que para que estas normas cumplan su objetivo, una vez el gobierno nacional la reglamente y las organizaciones las implementen, deben ser revisadas por la autoridad de protección, función que no fue enlistada en las funciones que se le van a asignar al mencionado ente."* (Sentencia C - 748, 2011)[48]

Ahora bien, para que estas herramientas sean vinculantes y efectivas, requieren de la voluntad y seriedad de las organizaciones, que sean acompañadas de herramientas internas y externas de verificación de cumplimiento tanto de procesos de certificación de calidad como de cumplimiento de estándares mínimos, contenga sanciones internas y externas que permitan determinar su eficacia. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

En pocas palabras, la autorregulación solo redunda en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento, de manera que se constituyan en meras declaraciones simbólicas de buenas intenciones, sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento de datos personales. (Angarita, Tratamiento de datos personales. Aproximacion internacional y comentarios a la ley 1581 de 2012, 2013)

[48] "Control de constitucionalidad al proyecto de ley estatutaria N° 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales" (Corte Constitucional. Sala plena. (M.P. Jorge Ignacio Pretelt Chaljub) 6 de Octubre de 2011).

V. CONCLUSIÓN

Los “datos personales” han cobrado cada vez mayor importancia en las actividades económicas y sociales, tanto del Estado como de los particulares. Se han convertido en un importante activo comercializable gracias a que muchos de los nuevos modelos de negocio se caracterizan por la utilización de información privada de los clientes para segmentar y personalizar ofertas, servicios y productos.

Las utilidades de las empresas dependen directamente del tratamiento de la información derivada de los datos personales como estrategia de venta, vulnerando los derechos fundamentales de las personas con el abuso del tratamiento de los datos toda vez que; primero, ofrecen múltiples posibilidades para “tratar” la información en poco tiempo y en la mayoría de las veces imperceptible para los titulares. Segundo, no cuentan con la seguridad necesaria para que esta información no sea utilizada de manera ilegal o poco ética. Tercero, estos mercados evolucionan rápidamente, haciendo cada vez más difícil que la regulación evolucione a la par. Y por último, pero el más importante, la transferencia internacional de los datos ha permitido el traspaso de las fronteras físicas, acelerando la circulación y recolección internacional de la información gracias al continuo crecimiento, haciendo cada vez mayor la cantidad de datos que se transfieren a través de países y continentes por los usuarios de internet, debido a la inmersión masiva de tecnologías de información y comunicación en el mundo.

Los medios de protección que facultan al titular en el ámbito internacional no son garantes, en la norma se habla de una clasificación del “nivel adecuado de protección” para garantizar

que al transferir los datos de un país a otro no se vulneren los derechos de los titulares, no obstante, en el plano internacional todavía no hay una normatividad global que aplique para todos sin importar el lugar de origen o donde finalmente se transfirieron los datos.

Se identificaron dos grandes sistemas que son la base de la regulación de los demás países, que además, tienen grandes diferencias no solo normativas sino ideológicas, donde Europa confía en el papel del Estado y tiene una concepción de protección de datos fundamentado en que el ciudadano es el propietario de sus datos y este cuenta con una autoridad de control, encargada de hacer cumplir la regulación, en la que se reconoce la protección de datos como un derecho fundamental. Contrapuesto a la concepción de Estados Unidos, quien confía en el individuo, limita al Estado y confía en la autorregulación del Mercado, fundamentada en una mezcla de legislación, reglamentación y autorregulación, donde no se reconoce la protección de datos como un derecho fundamental sino como un derecho al consumidor y a su vez carece de una autoridad de control.

En síntesis, mientras que el sistema Europeo lucha por prevenir la vulneración de los derechos fundamentales del sujeto como titular de los datos, Estados Unidos no busca prevenir sino resolver el conflicto en las cortes, compensando a posteriori cuando sea necesario.

Con el fin de subsanar las grandes diferencias entre estos dos modelos, que hacen que uno de ellos definitivamente no cuente con un nivel adecuado de protección de datos, se hace un llamado a la suscripción de acuerdos entre estados y la creación de sistemas de adhesión voluntaria, como el de los principios de puerto seguro. Sin embargo, EE.UU no logró asegurar la protección equivalente a la conferida por la UE, al presentar vicios que

conllevaron a su posterior anulación por la falta de transparencia y de control respecto a su efectiva aplicación.

Finalmente se puede concluir que otro de los factores influyentes para que a nivel internacional no se configure una efectiva protección de los titulares, es que las autoridades llamadas a vigilar y controlar, sólo están facultadas para actuar dentro de su territorio, una vez los datos estén fuera son responsabilidad de la autoridad o responsables del otro país, generando un vacío normativo y sin protección para los titulares de los datos, haciendo nuevamente evidente la necesidad de una normatividad global que cubra a todos los titulares independiente del país de origen y destino de los datos, y por ende la creación de una autoridad internacional imparcial que tenga facultades para vigilar, controlar y proteger el tratamiento de los datos personales.

REFERENCIAS

Angarita, N. R. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar Europeo? . *Revista Colombiana de Derecho Internacional*, 489 - 524.

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

Circular externa 005, "Adicionar un capítulo tercero al título V de la circular única" ((Superintendencia de Industria y Comercio 10 de Agosto de 2017).

Cuadrada, E. B. (2007). *La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reaccion frente a la vulneracion del derecho a la intimidad* . Revista de estudios de derecho y ciencia politica de la UOC N° 5.

Decreto 1377 , "Por el cual se reglamenta parcialmente la ley 1581 de 2012" (Presidente de la Republica 27 de Junio de 2013).

Ferrero, E. M., & Schutz, A. (2013). *"tráfico de datos personales: su afectación a los derechos personalísimos".* Obtenido de Biblioteca Unlpam: http://www.biblioteca.unlpam.edu.ar/rdata/tesis/e_fertra421.pdf

Franco, H. A. (2000). "La progresiva configuración de las transferencias de datos como objeto del tráfico comercial internacional". . *Sector exterior Español,,* 147 a 160 .

Gonzalez, A. G. (2007). “la protección de datos personales: derecho fundamental del siglo XXI un estudio comparado” . *Universidad latina de america*.

Ley Estatutaria 1581 , reglamentada parcialmente por el decreto Nacional 1377 de 2013. (Congreso de Colombia 17 de Octubre de 2012).

LouisD.Brandeis, & D.Warreny, S. (1890). *“The Right to Privacy”.* The Harvard Law Review,Vol.4,No.5.

Luque, J. M. (2002). *“Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: El sistema de principios de Puerto Seguro”.* Diario La Ley, nº 549.

Lusky, L. (1972). "Invasion of Privacy: a Clarification of Concepts". *Estado de derecho y Constitución,9a.ed.,,* 334-336.

Muñoz, R. G. (2016). *las transferencias internacionales de datos personales a Estados Unidos de América y la invalidez del régimen del Safe Harbour".* Barcelona: Monografía Universidad Autónoma de Barcelona.

NAÏR, S. (1 de Noviembre de 2013). *Imperialismo Digital* . Obtenido de EE UU usa la información para proteger su economía y el éxito depende de la pasividad de sus víctimas: http://internacional.elpais.com/internacional/2013/11/01/actualidad/1383333227_60524 3

Palazzi, A. (2003). *"Transferencia internacional de datos personales y armonización de leyes en un mundo globalizado".* Bogotá: Legis .

Rodriguez, F., & Julio, J. (s.f.). *"Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red",.* Instituto de Investigaciones Jurídica, Serie Doctrina Jurídica .

Rodríguez, M. Á. (1998.). *La protección de datos en Europa: principios, derechos y procedimiento* . Madrid : Grupo Asnef Equifax Universidad Pontificia de Comillas.

Rubio, A. E. (Noviembre de 2015). *"la cultura digital". " La era digital: cambio o revolución".* Obtenido de https://ined21.com/la-era-digital-cambio-o-revolucion/

Sentencia C - 1011 (Corte Constitucional. Sala plena. M.P. Jaime Córdoba Triviño 16 de Octubre de 2008).

Sentencia C - 748, Control de constitucionalidad al proyecto de ley estatutaria N° 184 de 2010 senado, 046 de 2010 Camara "por la cual se dictan disposiciones generales para la proteccion de datos personales. (Corte Constitucional. Sala plena MP Jorge Ignacio Pretelt Chaljub 6 de Octubre de 2011).

Sentencia T - 058, [M.P Luis Guillermo Guerrero Perez]. (Corte Constitucional, Sala Tercera de Revisión. 12 de Febrero de 2015).

Sentencia T - 729 (Corte Constitucional. Sala séptima de revisión. M.P. Eduardo Montealegre Lynett) 5 de Septiembre de 2002).

Valbuena, A. (s.f.). *"estudio sobre la aplicación de normas Colombianas sobre transferencia internacional de datos personales".* Bogota – Colombia.

Vicente Guasch Portas. (2014). *Las transferencias internacionales de datos en la normativa española y comunitaria, Agencia Española de Protección de Datos y Agencia Estatal* . Madrid: Boletín Oficial del Estado.

Constitución Política de Colombia 1991

Directiva 95/46/CE

Decisión 2001/497/CE

Decisión 2002/16/CE

Decisión 2004/915/CE

Organization for Economic Co – operation and Development, Declaration on Transborder Data Flows, adopted by the Governments of OECD Menber Countries on 8 October 1998 – C(98)177

Description of the safe Harbor Framework Although the respective sets of safe Harbor Privacy Principles, frequently asked questions and answers (FAQs), and enforcement statements of the two Safe Harbor Franmeworks are similar, they differ in a number of ways. Understanding the safe Harbor Frameworks requires familiarity with all the relevant documentos. http://export.gov/safeharbor/ue/index.asp