

**020100**

Bogotá, 07 de marzo de 2017

Doctor  
**PABLO FELIPE ROBLEDO DEL CASTILLO**  
Superintendente  
Superintendencia de Industria y Comercio  
Ciudad

**Asunto:** Comentarios a proyecto de Circular para  
adicionar un Capítulo Tercero al Título V de la Circular  
Única - Responsables y Encargados del Tratamiento de  
Datos Personales.

**Apreciado Superintendente,**

Reciba nuestro más cordial saludo. Inspirados en el bien común, en la democracia participativa y en la búsqueda del mayor desarrollo y bienestar social para los colombianos, nos permitimos presentar nuestros comentarios respecto al proyecto de la "Circular para adicionar un Capítulo Tercero al Título V de la Circular Única- Responsables y Encargados del Tratamiento de Datos Personales". Para estos comentarios, tomamos como base un análisis que se realizó con los diferentes actores del ecosistema digital en el tiempo disponible para este propósito.

## **I. Contexto Mundial y Colombia**

La competencia en los mercados de hoy es entre ecosistemas digitales, entendidos como la colaboración y combinación de actores públicos, privados, academia, emprendimiento y de financiación que permiten generar innovación en productos y servicios de economía digital. Estos ecosistemas se han vuelto un vehículo fundamental para generar empleo, inversión, exportación, hacer realidad la transformación digital de los modelos de negocio y particularmente para entrar en la economía con sus bienes y servicios al incluirlos en las cadenas globales de

valor<sup>1</sup>. En la práctica, gracias a la disrupción digital, lo que el Foro Económico Mundial denomina como la Cuarta Revolución Industrial<sup>2</sup>, se reducen los costos de información, y de su transmisión, a la vez que se amplía el acceso a más conocimiento y mejores comunicaciones. Una serie de condiciones que nos sitúa en un momento propicio para generar innovación en materia digital que nos lleva a construir puentes digitales que permitan conectar a Colombia con ecosistemas digitales y nuevos modelos de negocios, en lugar de elevar barreras que limiten nuestra capacidad para acceder y ofrecer, bienes y servicios digitales.<sup>3</sup>

El panorama en términos de demanda y volumen, en la adopción de las Tecnologías de la Información y las Comunicaciones (TIC) se dificulta ante decisiones que limiten la confianza en la apropiación de estas. Es ideal que los responsables de la formulación de políticas trabajen de manera cercana con el sector privado para lograr que el ambiente de negocios promueva la ciencia aplicada y el uso de las tecnologías emergentes. Colombia tiene el gran reto de pasar de ser una nación en etapa de Transición a una nación de Transformación Digital<sup>4</sup>. Esto requiere un cambio en la mentalidad del gobierno y de los empresarios en la forma en que entienden la regulación y su propósito, de tal manera que se promueva la era digital y se facilite la innovación en la sociedad como herramientas para impulsar el desarrollo y bienestar de todos. Por esto mismo, el freno digital que se desprende de imponer regulaciones restrictivas es un costo de oportunidad es enorme para toda la economía de Colombia, que quedaría rezagada frente al resto de competidores globales en cuanto a la apropiación de tecnologías.

El total de usuarios de internet a nivel global se ha triplicado en una década, es decir existen aproximadamente hoy 3,200 millones de personas que ya navegan en la red. Por otra parte, se estiman que existirán 25 Billones de "cosas" conectadas (IoT) en los hogares de países de OECD en el 2022. Este nutrido ecosistema, junto con herramientas de Big Data, Cloud Computing, Artificial Intelligence, Robótica y Open Data, entre otras, permitirá y facilitará el uso de Business Analytics para diseñar nuevos negocios y formular políticas públicas que estén en sintonía con las realidades de los modelos innovadores.

<sup>1</sup> "Fabricas Sincronizadas, América Latina y el Caribe en las cadenas globales de valor" BID, Juan Blyde, 2014

<sup>2</sup> "The Fourth Industrial Revolution, what it means, how to respond" WEF, <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>

<sup>3</sup> Digital Transformation Initiative, World Economic Forum, January 2017

<sup>4</sup> Informe de Desarrollo Mundial "Dividendos Digitales", Banco Mundial, 2016.

Por esto mismo, iniciativas como la que viene liderando el Departamento de Planeación Nacional (DNP) en materia de Big Data y de Data Analytics son tan oportunas. Tal y como lo afirma el Director del DNP, Simón Gaviria Muñoz, Colombia tiene una gran oportunidad “para obtener soluciones a problemas reales de los diferentes sectores de la industria”. Por ejemplo, con el SISBEN y gracias al Big Data se realizó un análisis que permitió cruzando dos bases de datos, el DNP detectó, en 2015, 653.000 casos de inconsistencias en el sistema<sup>5</sup>.

Por otra parte, se ha evidenciado un importante crecimiento del e-commerce en Colombia, por cuanto se estima que las transacciones por internet representan un 2,6% del PIB. De acuerdo con un estudio de Visa y Euromonitor, se calcula que en el 2015 las ventas en tiendas virtuales alcanzaron los US\$3.100 millones, lo que representa un crecimiento de 18% respecto de las ventas reportadas en el 2014 que ascendieron a US\$2.620 millones. Siguiendo esta tendencia, se anticipa un crecimiento de tal magnitud que las transacciones rodeen los US\$5.000 millones en 2018. Fenómenos como el Cyberlunes confirman el aumento y la confianza en el volumen de transacciones y pagos en línea.

A nivel mundial, gracias al acceso a internet, prácticamente no existe modelo de negocio que no utilice y se beneficie de la posibilidad de mover datos más allá de sus fronteras naturales<sup>6</sup>. La transferencia de datos no se limita al portafolio de las compañías TIC, sino por el contrario hace parte del “ADN” de cualquier empresa que quiere hacer negocios de manera eficiente y sin restricciones territoriales. Por esto mismo, cualquier regulación, normatividad e impuestos tienen que dimensionar y valorar el costo beneficio de su impacto<sup>7</sup> pues como lo afirma la OCED, en un contexto en que la economía digital crece todos los días, la regulación puede constituir barreras que impidan el desarrollo del comercio y la competencia.

En este sentido, la declaración ministerial de la OCDE en Cancún el año pasado sobre la economía digital (titulada: *Innovación, Crecimiento y Prosperidad Social de Cancún*) fue clara en sus objetivos, los cuales ya hacen parte de la hoja de ruta de todos los países miembros de este foro, y que por consiguiente se deben tener en

<sup>5</sup> “Colombia entra a las grandes ligas del Big Data”: Simón Gaviria Muñoz,  
<https://www.dnp.gov.co/Paginas/%E2%80%9CColombia-entra-a-las-grandes-ligas-del-Big-Data%E2%80%9D-Sim%C3%B3n-Gaviria-Mu%C3%B1oz-.aspx>

<sup>6</sup> “No Transfer, No Trade - the Importance of Cross-Border Data Transfers for Companies based in Sweden”,  
Olle Grönwald, Trade Policy Adviser, Swedish National Board of Trade, Presentation at CIFTIS, Beijing, 29  
May 2014

<sup>7</sup> Recommendation of the Council on Regulatory Policy and Governance, OECD, 2012

consideración y seguir con miras a la solicitud hecha por Colombia para formar parte de dicha organización.

Entre estos encontramos:

- Reducir las barreras a la inversión y a la adopción de tecnologías digitales en todos los sectores;
- Adoptar marcos tecnológicos neutrales que promuevan la competencia;
- Trabajar para establecer estándares técnicos globales que permitan la interoperabilidad y un internet seguro, estable, abierto y accesible;
- Desarrollar, en los más altos niveles de gobierno, estrategias para la privacidad y protección de datos, mientras se promueve al mismo tiempo el uso de datos, incluyendo datos del sector público;
- Utilizar procesos abiertos, transparentes e incluyentes para desarrollar la gobernanza global en internet;
- Reducir los impedimentos para el e-comercio nacional e internacional con políticas que fortalezcan la confianza de los consumidores y la seguridad de los productos;
- Mejorar la educación y la capacitación permanente para responder a la demanda de habilidades digitales y generales; y
- Aumentar el acceso al internet de banda ancha para cerrar las brechas a los servicios digitales<sup>8</sup>.

La competitividad y sostenibilidad de Colombia depende hoy y en su futuro de la productividad que tengan las empresas, lo cual se encuentra directamente relacionada con el fortalecimiento de los ecosistemas digitales regionales y su inserción en un mundo globalizado<sup>9</sup>. Actualmente, el Gobierno colombiano ha venido adelantando un conjunto de actividades estratégicas para convertirse en un *hub* de distribución de servicios de valor agregado, por ejemplo, servicios de TI y software a nivel regional, lo que va de la mano con la integración que está teniendo este país en escenarios como la Alianza del Pacífico.

Por esto mismo, el Ministerio de Comercio, Industria y Turismo, a través del Programa de Transformación Productiva (PTP), ha definido que "Industrias 4.0" es uno de los principales eslabones de las cadenas de valor a impulsar dentro de la política de desarrollo productivo, y en el CONPES 3866 (Política de Desarrollo

<sup>8</sup> Declaración Ministerial de la OCDE, Cancún, 2016 <https://www.oecd.org/sti/ieconomy/Digital-Economy-Ministerial-Declaration-2016-ESP.pdf>

<sup>9</sup> "Colombia Hacia un país de altos ingresos con movilidad social" Rafael de la Cruz, Leandro Gastón Andrián, Mario Loterszpil, BID, 2016

Productivo) se ha resaltado la importancia de la promoción de transferencia de conocimiento y tecnología, la innovación y el emprendimiento.

Sumado a los anteriores esfuerzos para construir puentes que permitan a Colombia continuar su proceso de integración internacional y de inmersión en la era digital, se encuentra también el trabajo que viene realizando ProColombia priorizando los planes de inversión y exportaciones de servicios en el sector software y TI en el país, por sus beneficios en materia de disponibilidad de capital humano calificado, conectividad y acceso a los mercados mundiales.

El artículo 333 de la Constitución Política claramente define la libre competencia como un derecho de todos que supone responsabilidades y establece que el Estado por *"mandato de la ley, impedirá que se obstruya o se restrinja la libertad económica"*. Lo anterior debe manifestarse en un interés del Estado por facilitar el desarrollo económico y sentar las bases para que todo empresario colombiano pueda competir adecuadamente, lo que en este panorama tecnológico depende de la capacidad de permanentemente compartir y recibir información para innovar en el diseño de nuevos productos y servicios, en función del progreso. Por esto mismo, la Superintendencia de Industria y Comercio, tiene dentro de sus más profundos pilares el de promover y facilitar el comercio, en el mejor interés de los consumidores colombianos.

En materia de economía digital una de las herramientas que más se utiliza, es el manejo de datos y por consiguiente surge la necesidad de acceder a software y tecnologías emergentes para optimizar la productividad, la gestión y el desarrollo de los negocios. Actualmente, los proveedores globales de servicios en este portafolio ofrecen todo tipo de soluciones para almacenar y recuperar datos a precios sumamente económicos, particularmente desde los Estados Unidos de América (E.E.U.U.), epicentro del desarrollo tecnológico. Así, ya no es necesario comprar costosas licencias para sacar provecho de aplicaciones y datos, pues las herramientas más sofisticadas del mundo están al alcance de cualquier compañía que, sin necesidad de invertir grandes cantidades en despliegue de infraestructura, puede acceder a estos servicios bajo distintas modalidades contractuales (como lo son Software As a Service, Data Center As a Service, Infraestructure As a Service, entre otras.).

## E.E.U.U.

Las aplicaciones en la actualidad, casi sin excepción, son diseñadas y se desarrollan para ser utilizadas por los usuarios a través de dispositivos móviles o de internet. Este tipo de aplicaciones, requieren de una infraestructura especial para

almacenar grandes cantidades de datos remotamente de tal forma que puedan nutrir la experiencia de sus a nivel mundial. Esta infraestructura es sumamente costosa y altamente sofisticada, razón por la cual grandes compañías del sector tecnológico han invertido billones de dólares en desarrollar la infraestructura y las plataformas necesarias para ofrecer servicios de almacenamiento remoto a clientes globales (algunos ejemplos son Amazon Web Services, Microsoft Azure, Oracle Cloud, IBM Cloud Services, Google Cloud, DigitalOcean, etc).

La participación de Colombia en la globalización está relacionada entre otras variables por su capacidad de aprovechar las economías de escala. Por esto mismo, existe una gran diferencia entre los servicios que presta un proveedor de "hosting en la nube" básico, y los servicios que presta un proveedor de punta de servicios en la nube. Los proveedores de servicios de punta y casi sin excepción se encuentran asentados en los E.E.U.U., por cuanto es dicho país el que ha desarrollado y lo continuara haciendo las tecnologías más modernas para atender las necesidades que permitan mejorar la productividad de cualquier modelo de negocio.

Teniendo en cuenta que son millones de clientes los que atienden los más grandes proveedores, cualquier empresa —por ejemplo, una PYME o un *startup* en Colombia— puede arrendar, por demanda, sin compromiso de permanencia alguna, espacio en servidores de las más altas sofisticaciones, por menos de lo que cuesta un salario mínimo en Colombia al mes. Con este dinero, la PYME o *startup* puede "hostear" su aplicación ofreciendo a sus clientes tecnología de punta, máximos niveles de seguridad y redundancia a fallas, entre otros valores agregados. Tener acceso a estas herramientas tecnológicas es un imperativo para cualquier empresa en Colombia que quiera competir tanto en el mercado local, como en los regionales y locales. En este sentido, eliminar del mercado a una gran cantidad de proveedores que tienen sus centrales de cómputo en E.E.U.U. es una afectación a la sana competencia, que implicaría un aumento desproporcionado en los costos de almacenamiento de datos, lo que podría reducir la capacidad de los colombianos de tener acceso a los nuevos desarrollos para ponerlos a los servicios de su productividad y de sus clientes.

De igual manera, el fomento de los emprendimientos de base tecnológica o "*startups*", que se dedican a desarrollar tecnologías disruptivas y de vanguardia con presupuestos muy bajos, se vería seriamente perjudicado por la regulación propuesta. Así, al enfrentarse a barreras regulatorias limiten el acceso a recursos tecnológicos, habrá cada vez menos insumos para el crecimiento de los *startups* colombianos, lo cual, junto con el incremento en costos, hará menos atractivo a Colombia para posibles inversionistas. En especial considerando que se excluirán

del mercado las soluciones informáticas más utilizadas, que proporciona un país como EEUU.

El mundo depende del software para moverse, por lo cual la velocidad, confianza y seguridad en los datos es esencial en cualquier actividad, pero especialmente para competir en mercados con tendencia hacia la globalización. En estas condiciones, los negocios eligen contratar ciertos servicios tecnológicos por razones que poco tienen que ver con su lugar de origen, y más con otras consideraciones como el precio, la calidad o una relación de ambas.

Por lo anterior, en Colombia se requiere hacer uso de herramientas tecnológicas extranjeras puesto que a) por su uso generalizado proporcionan mayores y mejores soluciones ante problemas técnicos, que se desprende de una larga tradición de uso, b) existen más extensiones, APIs, interconexiones, aplicativos, y en general recursos en ecosistemas más nutridos que el nuestro y c) el uso de software estandarizado y globalizado permite mayores relevancia a nivel mundial (tanto para empresas que quieran asociarse con otras extranjeras, o para aquellas que busquen competir a nivel mundial con base en Colombia).

A raíz de la revolución digital, especialmente en los últimos 10 años, las premisas técnicas bajo las cuales se diseñan aplicaciones han cambiado radicalmente. En el pasado, las compañías TIC alquilaban "espacio" físico en servidores dentro de un datacenter, o incluso alquilaban "metros cuadrados" dentro de los cuales desplegaban máquinas físicas (servidores). Este montaje podía ser realizado a pequeña escala dentro de Colombia sin mayores inconvenientes. Sin embargo, el licenciamiento requerido para operar aplicaciones bajo dichos anteriores era muy costoso. Antes, *hostear* una pequeña aplicación en la nube requería inversiones en licencias de US \$ 10,000 hasta US \$ 30,000 dólares, pues típicamente las licencias las aportaba quien construía la aplicación, no el datacenter. Así las cosas, *hostear* una aplicación robusta en la nube (por ejemplo, como Rappi, Tappsi, Mercadoni, Domicilios.com, etc.) podría llegar a costar al año más de US \$ 1 millón de dólares.

Actualmente se ha reducido de manera radical el costo asociado a los servicios de almacenamiento de datos. Una aplicación pequeña en internet construida por una *startup* se puede *hostear* en E.E.U.U. aproximadamente por menos de US \$300 dólares al mes, sin inversión de licenciamiento, pues todo se alquila. Una aplicación altamente robusta se puede *hostear* por menos de US \$ 50,000 dólares al año.

Consideramos que generar prohibiciones, establecer tramitologías o barreras que limiten el acceso a servicios en la nube basados en los E.E.U.U. sería nocivo para

la competitividad del aparato productivo colombiano y de empresas de servicios TIC, por cuanto la mayoría de aplicaciones que se construyen hoy en día dependen de servicios de computación en la nube (o son para consumo en móviles) que se encuentran en ese país. Los empresarios y consumidores colombianos, o clientes globales que las empresas TIC atienden, exigen que se utilicen plataformas de punta, de computación en la nube, para proveer la infraestructura que requiere la velocidad y seguridad de los negocios. Gracias a internet, las empresas hoy por hoy construyen aplicaciones multi-idioma, de alcance multinacional, que ante a los bajos costos y la facilidad de difusión pueden ser concebidas y operadas como una única y misma aplicación.

Un escenario similar se puede extender a cualquier necesidad de hardware, por cuanto la memoria de las máquinas es limitada. Por ejemplo, el número de usuarios puede crecer, los anchos de banda son insuficientes, etc., los cuales llevan a consideraciones y hechos que se solucionan con los proveedores de servicios en la nube. Estos ofrecen todo tipo de herramientas para convertir lo que era un enorme desafío en líneas de código que manejan el crecimiento del hardware, de cualquier tipo, de forma automática. Si el hardware crece, el modelo de servicio y de negocio se ajusta para cobrar por la utilización de más recursos, y solo por el tiempo que sean utilizados. En pocas palabras, las modalidades conocidas como “As a Service” permite mayor productividad a las empresas.

## II. Comentarios al Proyecto de Circular

Si bien la Ley 1581 de 2012 se formuló originalmente a partir de la necesidad legítima de salvaguardar los derechos de las personas sobre sus datos personales, los esquemas de protección de datos deben adaptarse a las circunstancias temporales. Por ende, no se puede perder de vista que actualmente, y cada vez más, el comercio es exponencialmente más global, lo cual hace indispensable un flujo constante de información transnacional.

Adaptarse a las rápidas dinámicas de los negocios es uno de los retos que enfrentan las empresas colombianas para entrar en cadenas globales de valor. No es conveniente limitar las posibilidades tecnológicas de progreso con barreras normativas, en lugar de escenarios más propicios para la innovación. Por ejemplo, las limitaciones pueden ser cambiadas por esfuerzos conjuntos con autoridades extranjeras, mediante los cuales se pueden aprovechar estas mismas eficiencias para idear mecanismos regulatorios más afines a las tecnologías emergentes.

La Superintendencia de Industria y Comercio, como su nombre lo dice, tiene dentro de sus más profundos pilares el de promover y facilitar el comercio, en el mejor



interés de los consumidores colombianos. Siendo esto así, negar que en el listado de países que proveen “adecuado nivel de protección de los datos personales” estén los principales países con los cuales el sector privado Colombia realiza comercio transfronterizo de bienes y servicios, así como intercambios Estado - Estado, significa un enorme muro legal para que ese dicho comercio continúe realizándose.

Consideramos que Colombia estaría enviando un mensaje equivocado sobre la mutua confianza que debe existir en las relaciones comerciales transfronterizas con los países que nos permiten una expansión económica basada precisamente en el intercambio transfronterizo. El sector privado colombiano se vería afectado, por una reducción en la productividad de sus empresas para exportar e importar. Igualmente, el sector público se vería rezagado por la imposibilidad de continuar beneficiándose de los productos proporcionados por compañías de países de tradición no europea.

Por otra parte, Colombia Compra Eficiente, como agencia principal para las compras públicas del Estado colombiano, que se encuentra adelantado el proceso de contratación del Acuerdo Marco de Precios de servicios de nube pública, ha manifestado preocupaciones el cambio regulatorio que traería el proyecto de circular materia de estos comentarios por cuanto queda en entredicho que las entidades públicas puedan acceder a los servicios de nube pública prestados por empresas regionales o globales.

La Ley 1581 le otorga a la Superintendencia de Industria y Comercio facultades para determinar el estándar o criterios para establecer los niveles adecuados de protección de datos personales, lo cierto es que no hace referencia a un único modelo (europeo) sino que le da suficiente campo a la entidad para que defina cuál es el mejor de los estándares, el que más conviene a Colombia y sus residentes y ciudadanos.

Precisamente porque la Ley de Datos Personales no limita y obliga a Colombia a adoptar los criterios y estándares europeos. Inclusive, la Superintendencia tiene la gran labor de evaluar todas las opciones (que la misma OECD ha reconocido como opciones válidas para garantizar el flujo transfronterizo de información) que están disponibles con el fin de que el país continúe facilitando el comercio transfronterizo con los países que son sus principales aliados comerciales, y con todos aquellos otros países que son aliados potenciales.

En principio, si nos quedamos en el marco jurídico europeo, vemos que la Unión Europea prevé un mecanismo específico para facilitar el intercambio de información personal con países por fuera de su modelo jurídico; es el caso del *Safe Harbor* o,

más recientemente, el *Privacy Shield*. Desafortunadamente, por la misma Ley 1581 de 2012, no es competente la Superintendencia para establecer el nivel de cumplimiento de estándares a compañías privadas específicas mediante mecanismos de autocertificación, como ocurre en estos dos acuerdos marco para envío de información, y se hace más necesario entonces acudir a otros modelos y mecanismos.

Dentro del mismo modelo europeo, otro mecanismo es el de las “Normas Corporativas Vinculantes” o Binding Corporate Rules (BCRs), y se trata de códigos corporativos que protegen la compartición de datos personales hecha bajo el amparo de tales códigos. Se trata, pues, de normas obligatorias para las empresas que los adoptan, y de la creación de mecanismos para que tales empresas puedan demostrar continuo cumplimiento con tales obligaciones ante las autoridades competentes de los países donde opere cada sede de la compañía. En Colombia, existe una provisión en la Ley 1581 que establece precisamente el deber del Ministerio del ramo y de la Superintendencia de Industria y Comercio de reglamentar dicho mecanismo e impartir instrucciones concienzudas que permitan que sea posible el intercambio de datos personales bajo tal otro esquema. No obstante, la reglamentación que se haga de este mecanismo no tiene la misma fuente legal que la determinación de estándares o criterios para determinar que un país cuenta con niveles adecuados de protección de datos personales, por lo que este mecanismo se convierte en una tarea adicional, y no que reemplace, la gestión fundamental de la Superintendencia de facilitar el envío de información y datos personales a países por fuera de la tradición europea.

Adicionalmente, es importante resaltar que el fundamento jurídico que tiene la Superintendencia para poder emitir e impartir instrucciones sobre cuáles son los criterios para definir los niveles adecuados de protección de datos personales, se encuentra dado por la Corte Constitucional colombiana que en sentencia C-748 de 2011 definió el alcance de aplicación del artículo 26 de la Ley 1581 con miras de ser exequible, diciendo que son dos los estándares requeridos para entender que ***“un país cuenta con los elementos o estándares de garantía necesarios para garantizar un nivel adecuado de protección de datos personales”***. ***Tales dos estándares son “si su legislación cuenta con unos principios, que abarquen las obligaciones y derechos de las partes (titular del dato, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos de datos personales), y de los datos (calidad del dato, seguridad técnica) y; con un procedimiento de protección de datos que involucre mecanismos y autoridades que efectivicen la protección de la información”***.

En esa medida, sugerimos que los estándares que establece la Superintendencia en la Circular sean replanteados de modo que la racionalidad económica y la

seguridad técnica como los primeros que determinen para dónde se dirige el derecho, teniendo siempre la protección de los residentes y ciudadanos colombianos como primer objetivo, lo cual implica que además de proteger su información personal, se proteja el acceso que éstos tienen, tanto como ciudadanos, como empresas y como estado, al intercambio económico con países como E.E.U.U. y como otros que están por fuera de Europa.

Por lo anterior, sorprende lo que propone el numeral 3.2 del Proyecto de Circular el cual presenta un listado de países que garantizan un nivel adecuado de protección según la Superintendencia por cuanto no se conoce si la SIC tuvo en cuenta cada uno de los estándares mencionados en el punto 3.1. del mismo proyecto de circular, solo algunos de ellos o si existe algún punto que prevalezca sobre los demás.

A su turno, en el listado de países que se identifican como aquellos que tienen un nivel adecuado de protección de datos personales, se excluye a E.E.U.U., el cual como mencionamos anteriormente cuando se habla de inserción en las cadenas globales de valor, la transferencia de datos transfronterizos entre países, modelos de negocio, empresas y personas que se realizan con E.E.U.U., es quizá una de las más intensas, frecuentes y modernas, las cuales requieren y tienen los más altos estándares de seguridad, protección y eficiencia para realizar el comercio de bienes y servicios con la economía más grande del mundo.

Generar un bloqueo a la transmisión de datos a E.E.U.U. tendría un impacto negativo en el crecimiento de la economía digital y las TIC. Soluciones de punta como *Blockchain* quedarían por fuera de las alternativas para construir una economía más moderna y competitiva. Para no afectar el mercado mundial, la SIC debe habilitar los flujos de datos transfronterizos, conservar la protección de los consumidores y promover la interoperabilidad de los datos.

Adicional a lo anterior, para contemplar un proyecto circular como esta, la SIC no puede dejar de lado los diferentes instrumentos, como el TLC entre Colombia y E.E.U.U., con base en los cuales los empresarios extranjeros han realizado inversiones a largo plazo, con el fin de incrementar su capacidad productiva y conservar condiciones favorables para sus negocios.

Específicamente, este tratado establece en el Capítulo 14 sobre Telecomunicaciones, artículo 14.2., numeral 3: *"Cada Parte garantizará que las empresas de otra Parte puedan usar servicios públicos de telecomunicaciones para mover información en su territorio o a través de sus fronteras y para tener acceso a la información contenida en bases de datos o almacenada de forma que sea legible por una máquina en el territorio de cualesquiera de la Partes"*.

La seguridad en los datos y la privacidad de la información exige a las compañías hacer uso de la mejor tecnología disponible para generarle confianza al consumidor digital y enfrentar los riesgos de ciberseguridad. Cada día el almacenamiento de información y datos de los usuarios aumenta, haciendo esta exigencia cada vez mayor. Por lo anterior, los gobiernos están obligados a ajustar sus marcos jurídicos, de manera que se facilite el desarrollo de plataformas y servicios digitales que faciliten la implementación de las mejores tecnologías para la protección de la información.

La gran mayoría de los países (incluyendo los de la Unión Europea, que tienen el régimen más estricto de protección de datos personales del mundo) ha adoptado un régimen de transferencia de datos personales al exterior. Colombia no es la excepción, tal y como lo estableció la ley 1581 de 2012 y lo reglamentó en el Decreto 1377 de 2013.

A manera de ejemplo, consideramos importante resaltar que en el documento titulado *"Beneficios Económicos y Sociales de la Apertura de Internet"*, de la OCDE, 2016, se establece que *"... Si bien algunos de los motivos detrás de la localización forzada de datos pueden ciertamente ser legítimos, esta hace a Internet más cerrada, puede no alcanzar los resultados esperados e incluso puede causar daños inesperados. Políticas de localización pueden restringir la apertura en la capa de infraestructura forzando a los negocios a usar centros de datos locales y/o medidas de enrutamiento, lo que restringe la competencia y en consecuencia la eficiencia. Las políticas de localización de datos pueden también restringir la apertura en la capa de aplicaciones cuando a las aplicaciones se les prohíbe usar o almacenar datos en el exterior. Todo esto restringe el libre flujo de información. Es más, la localización de datos no necesariamente lleva a una mayor privacidad y seguridad"*<sup>10</sup>.

- **Mecanismos de protección de datos en EE.UU.**

Con el objetivo de facilitar el análisis respecto a las normas que existen en E.E.U.U. que apliquen para al tratamiento de datos personales, presentamos a continuación algunos ejemplos:

Numerosas normas de privacidad federales y estatales han regulado la recopilación y el uso comercial de información personal. Citando a la Presidenta de la Comisión

<sup>10</sup> Traducción libre. El documento *"Economic and Social Benefits of Internet Openness"* de 2016 de la Organización Para la Cooperación y el Desarrollo Económicos-OCDE- se encuentra disponible aquí: [http://www.oecd-ilibrary.org/science-and-technology/economic-and-social-benefits-of-internet-openness\\_5jlwqf2r97g5-cn](http://www.oecd-ilibrary.org/science-and-technology/economic-and-social-benefits-of-internet-openness_5jlwqf2r97g5-cn).

Federal de Comercio de EE.UU. del momento, Edith Ramírez, tenemos que existen muchas normas “*más allá del artículo 5 de la FTC Act (Ley de la FTC)*”, incluyendo las siguientes: *Cable Communications Policy Act* (Ley de política de comunicaciones por cable), *Driver's Privacy Protection Act* (Ley de protección de la privacidad del conductor), *Electronic Communications Privacy Act* (Ley de privacidad de las comunicaciones electrónicas), *Electronic Funds Transfer Act* (Ley de transferencia electrónica de fondos), *Fair Credit Reporting Act* (Ley sobre imparcialidad de los informes de solvencia), *Gramm-Leach-Bliley Act* (Ley Gramm-Leach-Bliley), *Right to Financial Privacy Act* (Ley del derecho a la privacidad financiera), *Telephone Consumer Protection Act* (Ley de protección del consumidor de telefonía) y *Video Privacy Protection Act* (Ley de protección de la privacidad de video). Muchos Estados también contaban con leyes análogas en estos ámbitos”<sup>11</sup>.

Tal como se lee en el Apéndice A de la Carta de Presidenta de la Comisión de Federal de Comercio, entregada a la Comisión Europea e incorporada como Anexo IV a la Decisión de Adecuación del Escudo de Privacidad, complementamos diciendo que:

*“desde 2000, se han producido numerosos avances, tanto a nivel federal como a nivel estatal, que establecen protecciones adicionales para la privacidad de los consumidores. A nivel federal, por ejemplo, la FTC modificó el Reglamento COPPA en 2013 para introducir varias protecciones adicionales a la información personal de los menores de edad. Asimismo, la FTC emitió dos normas de aplicación de la Ley Gramm-Leach-Bliley —la Regla de privacidad y la Regla de salvaguardias— que exigen que las instituciones financieras efectúen revelaciones sobre sus prácticas de intercambio de información y apliquen un programa integral de seguridad de la información para proteger los datos de los consumidores. Asimismo, la Fair and Accurate Credit Transactions Act («FACTA») (Ley de Transacciones de Crédito Justas y Exactas), promulgada en 2003, complementa a las antiguas leyes estadounidenses sobre el crédito estableciendo requisitos para el enmascaramiento, el intercambio y la eliminación de determinados datos financieros confidenciales. La FTC ha promulgado varias normas con arreglo a la FACTA relativas, entre otras cosas, al derecho de los consumidores a un informe de crédito anual gratuito; los requisitos de eliminación segura de los datos de informe de los consumidores; el derecho de los consumidores a anular la recepción de determinadas ofertas de crédito y seguros; el derecho de los consumidores a cancelar el uso de información proporcionada por una empresa filial para comercializar sus productos y servicios; y requisitos para las instituciones financieras y los acreedores para que apliquen programas de detección y*

<sup>11</sup> Apéndice a la Carta de la Presidenta de la Comisión Federal de Comercio de EE.UU. a la Comisión Europea, fechada 7 de julio de 2016.

*prevención del robo de identidad. Además, las normas promulgadas en virtud de la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario se revisaron en 2013 añadiendo medidas adicionales para proteger la privacidad y la seguridad de la información personal sobre salud. También han entrado en vigor normas que protegen a los consumidores contra llamadas de marketing telefónico no deseadas, llamadas telefónicas automáticas y recepción de correo basura. El Congreso también ha promulgado leyes que exigen a ciertas empresas que recopilan información de salud que envíen a los consumidores una notificación en caso de incumplimiento". (...)*

Finalmente, debe destacarse lo relacionado con la Ley de Libertad de EE.UU., promulgada en junio de 2015, que, entre otras cosas: "(...) *Prohíbe la recopilación en bloque de los registros, incluidos los de los ciudadanos estadounidenses y los de los no estadounidenses, de conformidad con las disposiciones de la FISA o mediante el uso de las Cartas de Seguridad Nacional, una forma de citaciones administrativas autorizadas por ley* (6)<sup>12</sup>".

A estas normas se suman decenas de normas estatales que regulan distintos aspectos de la privacidad en EE.UU.

- **Consagración normativa de principios aplicables al Tratamiento de datos, en otros: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.**

En las decenas de normas de privacidad que existen en EE.UU. se consagran reiteradamente los principios de administración de datos personales, siguiendo los estándares internacionales. Sería imposible hacer una enumeración completa de estas consagraciones, por lo que nos limitamos a dar unos pocos ejemplos:

1. En el Apéndice A citado anteriormente se hace referencia al principio de temporalidad en las transacciones financieras: "*Asimismo, la Fair and Accurate Credit Transactions Act («FACTA») (Ley de Transacciones de Crédito Justas y Exactas), promulgada en 2003, complementa a las antiguas leyes estadounidenses sobre el crédito estableciendo requisitos para el enmascaramiento, el intercambio y la eliminación de determinados datos financieros confidenciales. La FTC ha promulgado varias normas con arreglo a la FACTA relativas, entre otras cosas, al derecho de los consumidores a un*

<sup>12</sup> Carta del Asesor General, Robert Litt, Director de la Oficina del Director de Inteligencia Nacional al Departamento de Comercio de EE.UU.

*informe de crédito anual gratuito; los requisitos de eliminación segura de los datos de informe de los consumidores; el derecho de los consumidores a anular la recepción de determinadas ofertas de crédito y seguros; el derecho de los consumidores a cancelar el uso de información proporcionada por una empresa filial para comercializar sus productos y servicios”.*

2. En temas de uso de información para fines de inteligencia, encontramos claras consagraciones al principio de finalidad y a los principios de necesidad y proporcionalidad: *“Limitaciones: de conformidad con la Constitución de los Estados Unidos de America, corresponde al presidente, en su calidad de jefe de Estado y de Gobierno y capitán general de las Fuerzas Armadas, garantizar la seguridad nacional y, por lo que respecta a la inteligencia exterior, administrar los asuntos exteriores del país. Si bien el Congreso está facultado para imponer limitaciones, y así lo ha hecho en diversos aspectos, el presidente podrá dirigir dentro de estos límites las actividades de los servicios de inteligencia estadounidenses. (...) Por último, aun cuando los Estados Unidos consideren necesaria la recopilación indiscriminada de inteligencia de señales, en las circunstancias previstas en los considerandos 70 a 73, la PPD-28 limita el uso de dicha información a una lista específica de seis fines de seguridad nacional destinados a proteger la privacidad y las libertades civiles de todas las personas, con independencia de su nacionalidad o su lugar de residencia (74). Estos fines admisibles comprenden medidas para detectar y neutralizar las amenazas que plantean el espionaje, el terrorismo, las armas de destrucción masiva y las amenazas de ciberseguridad para las Fuerzas Armadas o el personal militar, así como las amenazas delictivas transnacionales relacionadas con los otros cinco fines, y se revisarán con una periodicidad mínima anual. De las declaraciones del Gobierno estadounidense se desprende que los servicios de inteligencia han reforzado sus prácticas analíticas y sus normas para consultar la inteligencia de señales no evaluada con arreglo a estos requisitos; el empleo de consultas específicas garantiza que únicamente se presenten a los analistas, para su examen, los elementos que se considera que podrían aportar información valiosa. Aunque no se formule en tales términos jurídicos, estos principios captan la esencia de los principios de necesidad y proporcionalidad. Se concede una clara prioridad a la recopilación selectiva, mientras que la recopilación indiscriminada se limita a situaciones (excepcionales) en las que no es posible llevar a cabo una selectiva por motivos técnicos u operativos. Aun cuando no pueda evitarse la recopilación indiscriminada, el acceso a tales datos y su posterior utilización se limita estrictamente a fines legítimos y específicos de seguridad nacional”.*

- **Existencia de autoridad (es) pública (s) encargada (s) de la supervisión del Tratamiento de datos personales, del cumplimiento de la legislación aplicable y de la protección de los derechos de los titulares.**

Múltiples autoridades materializan los anteriores principios y se encargan del cumplimiento de las normas que protegen los datos personales en EE.UU. A manera de ejemplo, valga citar nada más una corta descripción de las funciones de la FTC: *"La FTC es la principal agencia de protección del consumidor en EE. UU. especializada en la privacidad del sector comercial. La FTC tiene autoridad para enjuiciar los actos o prácticas desleales y engañosos que violan la privacidad de los consumidores, así como para hacer cumplir leyes de privacidad más específicas que protegen determinados datos financieros y sanitarios, la información sobre los menores de edad y la información utilizada para tomar ciertas decisiones de idoneidad sobre los consumidores. La FTC tiene una amplia experiencia en la aplicación de las leyes de privacidad de los consumidores. Las acciones coercitivas de la FTC se han ocupado de prácticas ilegales tanto en contextos fuera de línea como en línea... Los autos dictados contra estas empresas han dado lugar en general a un control continuo por parte de la FTC durante un período de veinte años, han prohibido nuevos incumplimientos de las leyes y han impuesto importantes sanciones financieras a las empresas por el incumplimiento de los autos. Cabe destacar que los autos de la FTC no solo protegen a las personas que hayan denunciado un problema; también protegen a todos los consumidores que tengan relación con las empresas en el futuro. En el contexto transfronterizo, la FTC tiene competencia para proteger a los consumidores de todo el mundo contra prácticas que se lleven a cabo en EE. UU."*

- **c) Existencia de medios y vías judiciales y/o administrativas para garantizar la tutela de los derechos de los Titulares y exigir el cumplimiento de la ley.**

Nuevamente, sería extremadamente dispendioso citar todos los mecanismos judiciales y administrativos que existen en el derecho de EE.UU. en materia de protección de datos personales. A manera de ejemplo, baste esta cita del Considerando 111 de la Decisión de Ejecución (UE) 2016/1250 DE LA COMISIÓN de 12 de julio de 2016: *"El Derecho estadounidense pone una serie de vías de recurso a disposición de los interesados de la UE que alberguen dudas sobre si sus datos personales han sido tratados (entre otros, mediante su recopilación o el acceso a los mismos) por los servicios de inteligencia de los Estados Unidos y, de ser así, si se han respetado las limitaciones previstas en tal Derecho. Estas se refieren básicamente a tres ámbitos: las injerencias previstas en la FISA; el acceso*



intencionado y no autorizado a datos personales por funcionarios públicos; y el acceso a información en virtud de la Freedom of Information Act (Ley de Libertad de Información; en lo sucesivo, FOIA. En primer lugar, la FISA contempla una serie de recursos, también a disposición de los ciudadanos no estadounidenses, para impugnar la vigilancia electrónica ilegal. Esto incluye la posibilidad para las personas de interponer una demanda de indemnización por daños y perjuicios económicos contra los Estados Unidos cuando se haya utilizado o divulgado información sobre ellas de manera intencionada y no autorizada; de demandar a funcionarios públicos estadounidenses a título personal («con apariencia de legalidad») por daños y perjuicios económicos; y de impugnar la legalidad de la vigilancia (y solicitar la supresión de la información) en el supuesto de que el Gobierno de los Estados Unidos pretenda utilizar o divulgar cualquier información obtenida o derivada de la vigilancia electrónica en contra del interesado en diligencias judiciales o administrativas emprendidas en dicho país. En segundo lugar, el Gobierno estadounidense indicó a la Comisión una serie de vías adicionales que los interesados de la UE podían utilizar para presentar un recurso contra determinados funcionarios por el acceso no autorizado a datos personales y la utilización de estos por parte el Gobierno, incluso con presuntos fines de seguridad nacional [a saber, la Computer Fraud and Abuse Act (Ley de Abuso y Fraude Informático); la Electronic Communications Privacy Act (Ley de Privacidad de las Comunicaciones Electrónicas) (163); y la Right to Financial Privacy Act (Ley del Derecho a la Confidencialidad Financiera). Todos estos fundamentos jurídicos para incoar un procedimiento se refieren a datos, objetivos o tipos de acceso específicos (por ejemplo, el acceso remoto a un ordenador a través de Internet) y pueden invocarse en determinadas circunstancias (tales como la comisión de actos intencionados o premeditados, o actos al margen de las propias funciones, así como el padecimiento de daños) (165). La Administrative Procedure Act (Ley de procedimiento administrativo) ofrece una posibilidad de recurso más general (título 5, artículo 702 del USC) según la cual toda persona que sufra un perjuicio a causa de actuaciones de una agencia o que se haya visto adversamente afectada o perjudicada por la acción de una agencia, tiene derecho a interponer un recurso judicial. Esto incluye la posibilidad de solicitar al órgano jurisdiccional que declare ilegales y anule la actuación, los resultados y las conclusiones de la agencia que hayan resultado ser arbitrarios, caprichosos, un abuso de la facultad de apreciación, o de otro modo no conformes a Derecho”.

- **Consagración normativa de deberes de los Responsables y Encargados.**

Conforme lo mencionamos atrás, todas y cada una de las normas que rigen el tratamiento de datos en EE.UU. establecen obligaciones precisas para las

empresas que administran información personal, con lo que se hace evidente el cumplimiento de este requisito.

Una vez presentado el contexto mundial y de Colombia en materia de economía digital, con sus retos y oportunidades, y a la vez aportando algunos elementos normativos que permiten conocer el adecuado marco jurídico en materia de protección de datos personales en EEUU, solicitamos respetuosamente:

1. Incluir en el numeral 3.2. de la Circular a los Estados Unidos de América
2. Redefinir los criterios en el numeral 3.1 de la Circular, con el fin de incorporar en este otros países y jurisdicciones. Proponemos, en este sentido, los siguientes criterios para el numeral 3.1 mencionado:
  - a) Existencia de normas aplicables al tratamiento de datos personales.
  - b) Existencia de principios aplicables al Tratamiento de datos.
  - c) Consagración normativa de derechos respecto de los datos.
  - d) Consagración normativa de deberes de quienes realicen el tratamiento de datos.
  - e) Existencia de procedimientos para garantizar la protección de la información o de la privacidad, los cuales podrán ser administrativos, judiciales, extrajudiciales o privados.
  - f) Existencia de una o varias autoridades(es) encargada(s) de protección de datos personales o de privacidad".
3. Adicionar en el parágrafo 3.2 consulta a la SIC en caso de inquietudes frente al cumplimiento de países no incluidos en la lista
4. Nos indiquen si se realizó un estudio para identificar los países con nivel adecuado de protección de datos. De ser afirmativo, agradecemos nos envíe el documento que contenga los criterios, elementos y estándares que llevaron a calificar el nivel adecuado de los países en la protección de datos.

Reiteramos nuestro interés de reunirnos nuevamente con Usted y su equipo de trabajo para discutir urgentemente las anteriores preocupaciones con el objetivo de



aportar en el análisis respectivo de manera que se logre construir un ambiente jurídico sólido, estable y competitivo para el desarrollo de las Industrias 4.0.

La disrupción digital y el desarrollo exponencial de tecnologías emergentes identificadas por el Foro Económico Mundial como manifestaciones de la cuarta revolución industrial, trae retos y oportunidades para los gobiernos y el sector privado. El costo de oportunidad aumenta al no facilitar la evolución digital, mediante una regulación y normatividad que permita mayor inclusión e interconexión de modelos de negocio y servicios entre el estado y el sector privado.

Cordialmente,

  
**SANTIAGO PINZÓN GALÁN**

Vicepresidente de Transformación Digital