Bogotá, marzo 8 de 2017.

Doctora
MARÍA CLAUDIA CAVIEDES
Superintendente Delegada
Delegatura de Protección de Datos
Superintendencia de Industria y Comercio (SIC)

Respetada doctora Caviedes:

Desde el GECTI –***G**rupo de **E**studios en internet, **C**omercio electrónico, **T**elecomunicaciones e **I**nformática-* https://gecti.uniandes.edu.co y el Observatorio CIRO ANGARITA BARÓN sobre la protección de datos en Colombia https://habeasdatacolombia.uniandes.edu.co, nos permitimos compartirle nuestra opinión sobre el proyecto de circular externa que tiene por objeto: "Impartir instrucciones a los Responsables y Encargados del Tratamiento de datos personales respecto de la transferencia y transmisión de datos a terceros países."

Nos parece positivo el trabajo que la SIC ha iniciado con la expedición del proyecto de circular sobre transferencias internacionales de datos.

Esta opinión personal, mis reflexiones y solicitudes las estructuro de la siguiente manera:

Contenido

1. De la importancia de la transferencia internacional de datos personales (TIDP)

La transferencia de información entre países con diferentes culturas jurídicas es una realidad que tiende a continuar creciendo a medida que se incrementan las relaciones sociales y económicas junto con el aumento de usuarios de internet y la inmersión masiva de las TIC en el mundo[1]. Vivimos en una sociedad globalizada e interconectada tecnológicamente en donde internet ha facilitado significativamente las posibilidades de intercambio de información[2].

Los procesos de integración económica ponen de presente la necesidad de exportar e importar[3] datos personales entre las empresas privadas, las personas o las autoridades de los diferentes países. De hecho, se ha reconocido que estos procesos han aumentado significativamente los flujos transfronterizos de datos[4] y que fue necesario expedir normas sobre tratamiento de datos que conciliaran la protección de la privacidad y la transferencia internacional de datos.

[1] En 1980 la OCDE reconocía que la circulación de datos "se ha incrementado en gran medida en años recientes y que van a aumentarse aún más con la introducción generalizada de nuevas tecnologías de informática y de comunicaciones" (Parte tomada del prólogo del siguiente documento: OCDE. 1980. *Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales*)

[2] Cfr. DE TERWANGNE, Cécile. 2009. Is a Global Data Protection Regulatory Model Possible?, en Reinventing data protection?, editado por S. GUTWIRTH. Netherlands: Springer. P. 177. Esta autora denomina nuestra sociedad como "the globalized and networked society"

[3] En este sentido señala la doctrina que la globalización de las actividades económicas ha intensificado los procesos transfronterizos de intercambio y circulación de información. [DE TERWANGNE, op. cit., p. 17.]

[4] Cfr. Numeral 4 de los considerandos de la Directiva 95/46/CE.

Diversas son las razones por las cuales las empresas, las personas naturales y los gobiernos requieren transferir datos personales a otros países o recibir esa información proveniente de otras partes del mundo. En el caso de los Estados es recurrente justificar la transferencia internacional de datos por motivos de seguridad pública, seguridad nacional, investigaciones contra el terrorismo, labores de inteligencia militar o policial, cooperación judicial, cooperación internacional en general, protección de un interés del titular del dato, controles de inmigración, entre otros.

En el plano empresarial, las multinacionales requieren circular información entre las diferentes sucursales o establecimientos que poseen a lo largo del planeta[5]. Otras empresas necesitan de la misma para brindar atención telefónica a los clientes a través del *call centers* internacionales, realizar acciones de *marketing*, administrar, proveer y dar soporte técnico a las bases de datos de clientes y proveedores, tener un perfil lo más completo posible sobre un potencial cliente[6] y realizar procesos de "*big data*".

[5] Sobre la necesidad de exportar información para diferentes fines véase: PEREZ ASINARI, María Verónica. 2003. *The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-commerce Context?.* Conferencia presentada en el 18th BILETA Conference: Controlling Information in the Online Environment. Lóndres, Reino Unido: Queen Mary & Westfield College, University of London

[6] La gran mayoría de los ejemplos fueron tomados de la presentación titulada "*Globalización de la privacidad: hacia unos estándares comunes –transferencias internacionales de datos*-"de María José BLANCO, Subdirectora General del Registro General de Protección de Datos de la Agencia Española de Protección de Datos. La conferencia tuvo lugar durante el VI encuentro Iberoamericano de protección de datos realizado en Cartagena de Indias (Colombia) del 27 al 30 de mayo de 2008.

El valor y la utilidad de los datos personales dependen, en muchos casos, de su posibilidad de circulación internacional en la medida que puedan ser entregados o remitidos a terceros para diversos propósitos. Una de las originarias situaciones que abordaron las normas sobre tratamiento de datos personales fueron las transferencias de naturaleza transfronteriza o internacional, estableciendo pautas para permitir que los datos tratados en un país puedan ser enviados a otro.

2. De los paraísos informáticos al principio de continuidad de protección de datos en las TIDP

Muchos países del mundo carecen de normas sobre tratamiento de datos lo cual significa que en esas partes del planeta no existe certeza sobre la forma de proteger los derechos de los titulares de los datos o simplemente no se protege a las personas frente al tratamiento indebido de los datos personales. En la nota explicativa[7] del Convenio 108 del Consejo de Europa[8], de 28 de enero de 1981, se reconoció la existencia de países que no tienen leyes de protección de datos o que las tienen pero con niveles bajos de protección denominados "paraísos informáticos" (data havens) en donde la protección de los derechos de los titulares de los datos es débil o inexistente.

[7] El texto de la nota (explanatory report) puede consultarse en: http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm

[8] La versión oficial del Convenio se encuentra publicada en: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I.1981

Palazzi, refiriéndose al artículo 25 de la Directiva 95/46/CE comenta que la finalidad de dicha norma es "evitar la creación de paraísos informático (*data havens*), es decir, jurisdicciones donde la carencia de leyes de protección de datos, las transforme en sitios atractivos para realizar tratamientos de datos personales que pueden ser violatorios de otras leyes de privacidad"[9] Los "paraísos informáticos" no sólo comprenden países sin regulación sobre tratamiento de datos personales sino que también cobija otros temas como, entre otros, los delitos informáticos. Para la ONU, por ejemplo, los "paraísos informáticos" son "estados que no dan prioridad a la reducción o prevención del uso ilícito de las redes de computadoras, o donde no se han elaborado leyes de procedimiento eficaces"[10].

Las TIC e Internet[11] permiten a las personas realizar muchas actividades desde cualquier parte del mundo. Así las cosas, para ellas puede ser conveniente, en ciertos casos, seleccionar países en donde no exista legislación sobre la actividad lo cual les permite obrar libremente y mitigar cualquier riesgo jurídico de ser investigados o sancionados por incumplir la ley del país que escogieron como domicilio[12]. En este sentido, la ONU destaca que "las estructuras abiertas de las

[9] Cfr. PALAZZI, Pablo. 2003. Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado. En Derecho de internet & telecomunicaciones, editado por GECTI. Bogotá: Legis. p 299

[10] Cfr. ORGANIZACIÓN DE LAS NACIONES UNIDAS. 2000. Delitos relacionados con las redes informáticas. Documento A/CONF.187/10 sobre antecedentes para el curso práctico sobre delitos relacionados con las redes informáticas. En Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. Viena: ONU. p 3.

[11] Señala Palazzi que "no es necesario aclarar que con el explosivo desarrollo de Internet y la velocidad y la facilidad de las comunicaciones actuales, la posibilidad de encontrar data havens es cada vez más alta" [Cfr. PALAZZI, 2003, op. cit., p. 299]

[12] Para la ONU, en el campo de los delitos informáticos, "los delincuentes cibernéticos pueden encauzar sus actividades electrónicas a través de un determinado Estado en el

redes informáticas internacionales ofrecen a los usuarios la oportunidad de elegir el entorno jurídico que mejor se ajuste a sus propósitos. Los usuarios pueden elegir un país en el que determinadas formas de comportamiento que puedan desarrollarse en un entorno electrónico no se hayan tipificado como delitos. Esto puede atraer la actividad de personas de otros Estados en cuyos ordenamientos jurídicos esas mismas actividades constituyan un delito" [13].

En los medios de comunicación se ha puesto de presente la problemática que generan a las autoridades dichos paraísos. En efecto, según las autoridades españolas, "las unidades de policías especializadas en perseguir los delitos informáticos consideran que el principal problema para luchar contra este tipo de criminalidad son los "paraísos informáticos", países donde la falta de legislación y de control en ese campo sirve de "punta de lanza" a estos delincuentes"[14]. Particularmente se recalca que "el delincuente sabe que ´hay países donde hay una legislación muy laxa´ en esta materia y que le permite ´ampararse y acudir a estos paraísos informáticos como punta de lanza o camino´ para cometer sus delitos, y ha precisado que este problema es "muy preocupante" en países de Europa del Este y Asia. De este modo, y después de una investigación minuciosa,

---

que ese comportamiento no esté tipificado como delito y por lo tanto quedar amparados por las leyes de ese país" [Cfr. ONU, 2000, op. cit., p. 5.]

[13] Ibíd., p. 3.

[14] Cfr. Los 'paraísos informáticos', la mayor pesadilla de los 'ciberpolicías'. Los países sin legislación ni control sirven de 'punta de lanza' a estos delincuentes. Noticia publicada por el diario el mundo.es el 22 de octubre de 2007 en su página web http://www.elmundo.es/navegante/2007/10/22/tecnologia/1193064956.html (última consulta Junio 15 de 2014)

´cuando llegamos a ese país, no hay nada que hacer´"[15]. Este panorama en materia de delitos informáticos puede replicarse al caso del tratamiento de datos personales.

Vista la gravedad potencial de esta realidad, en materia de tratamiento de datos se han establecido reglas para evitar que los datos objeto de transferencias internacionales lleguen a "paraísos informáticos". En efecto, a partir de los documentos analizados puede establecerse que, como regla, para que se permita transferir datos de un país a otro se debe verificar que el país receptor de los mismos garantice un nivel "adecuado" de protección de los datos personales. "Adecuado" inicialmente se refiere a que el país en donde se reciban los datos exista un grado de protección superior, igual, similar o equivalente al del país desde donde se remiten los mismos.

Con lo anterior se busca evitar que con ocasión de una operación de exportación de datos personales se disminuya el nivel de protección que se le garantiza al titular del dato en el país exportador. En otros términos, se quiere que el nivel de protección del país exportador se garantice en el país importador. Esta regla es conocida como el principio de continuidad de la protección de datos y se fundamenta en que "*la transferencia internacional de datos no debe afectar la protección de los interesados por lo que respecta al tratamiento de sus datos personales*"[16]. Así las cosas, en diversos documentos internacionales y la ley 1581

[15] Loc. cit.

[16] Cfr. DE FRUTOS, JOSÉ MANUEL, "*Globalización de la privacidad: hacia unos estándares comunes*", Conferencia presentada dentro del marco del VI encuentro Iberoamericano de

de 2012 se han establecido reglas y mecanismos para procurar garantizar el citado principio de continuidad.

3. Hacia una transferencia internacional responsable de la efectividad de los derechos de los titulares de datos personales privados, semiprivados y sensibles.

La ley 1581 de 2012, por regla general, prohíbe tres cosas:

(i) El tratamiento de datos sensibles (artículo 6);
(ii) El tratamiento de datos privados, semiprivados y sensibles de los menores de edad (artículo 7), y
(iii) "*la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos*" (Artículo 26).

Las anteriores prohibiciones no son absolutas ya que excepcionalmente pueden desconocerse si se cumplen unos requisitos previstos en el ordenamiento jurídico. La ley 1581 de 2012 y sus decretos reglamentarios, por ejemplo, establecen las condiciones jurídicas para que puedan realizarse transferencias y transmisiones de datos personales a otros países.

Ni los Estados ni los particulares están obligados a sacar o exportar los datos personales del territorio colombiano. Y si lo hacen, deben responsabilizarse de la efectividad de los derechos de los titulares de los datos cuya información exportan desde Colombia a otras partes del mundo. En otras

Protección de Datos realizado en Cartagena de Indias (Colombia) del 27 al 30 de mayo de 2008.

palabras, el exportador del dato personal no debe desentenderse el respecto de los derechos de las personas por el simple hecho de enviar información de terceros a otros países. De permitirlo, se avalaría la transferencia irresponsable de los datos personales privados, semiprivados y sensibles de las colombianas y los colombianos.

Existen varias razones jurídicas para afirmar que enviar datos personales fuera del país pone en mayor riesgo la posibilidad de garantizar la plena observancia del derecho al habeas data de los colombianos y expone a los (as) colombianos (as) a otros riesgos de tipo jurídico y político por el mero hecho de salir su información fuera del país.

4. De los riesgos que el tratamiento de datos en el extranjero podría causar sobre los derechos de los (as) colombianos (as).

Varias cosas deben tenerse en cuenta:

a) Inaplicabilidad de la ley colombiana, sometimiento de los colombianos a leyes y jueces extranjeros y no garantía plena del derecho fundamental a la protección de datos personales

Cuando los datos son tratados por empresas extranjeras no domiciliadas en Colombia, las colombianas y los colombianos se someten a la ley y a los jueces de otros países. Así por ejemplo, si un usuario colombiano tiene una disputa con Facebook, la misma se regirá por la ley del Estado de California de los Estados Unidos y únicamente será competente un tribunal del Distrito Norte de California o en un tribunal estatal del Condado de San Mateo[17]. Así las

[17] En efecto, el numeral 15 de las políticas de Facebook dice lo siguiente: *"Disputas. Resolverás cualquier demanda, causa de acción o conflicto (colectivamente, "demanda") que tengas con nosotros surgida de o relacionada con la presente Declaración o con*

cosas, este tipo de disposiciones contractuales de empresas extranjeras impide que se garantice plenamente el derecho fundamental al habeas data como se protegería en la República de Colombia.

En otras palabras, una vez los datos salen del país prácticamente desaparece la protección que el Estado colombiano otorga a las personas y los ciudadano quedan sometidos a un mundo de incertidumbre sobre la protección real y efectiva de sus datos.

b) Pérdida de control de la información.

Al salir los datos del territorio colombiano se pierde control sobre la información por parte del titular del dato y el Estado colombiano.

La información exportada queda sujeta a las regulaciones y autoridades de otros países. Los derechos de los titulares quedan en manos de la buena voluntad de la empresa u organización receptora de los datos que se encuentra ubicada en otro país. Esto es paupérrimo es insuficiente para garantizar la efectividad de los derechos de las personas frente a la circulación transfronteriza de los datos personales.

Facebook únicamente en el tribunal del Distrito Norte de California o en un tribunal estatal del Condado de San Mateo, y aceptas que sean dichos tribunales los competentes a la hora de resolver los litigios de dichos conflictos. Las leyes del estado de California rigen esta Declaración, así como cualquier demanda que pudiera surgir entre tú y nosotros, independientemente de las disposiciones sobre conflictos de leyes.". Cfr. https://www.facebook.com/legal/terms (Última consulta: 28/XII/2016 a las 9:39 AM hora local colombiana)

c) Sumisión de los colombianos a las decisiones de las autoridades o gobiernos de otros países: de la Executive Order: Enhancing Public Safety in the Interior of the United States del 25 de enero de 2017

Al estar los datos de los colombianos en data centers o equipos ubicado fuera del territorio colombiano, la información contenida en los mismos puede ser eventualmente accedida o conocida por las autoridades de otros países. Esto es así porque cada país tiene sus propias normas que obligan a las empresas domiciliadas en los mismos y sus autoridades pueden emitir órdenes de acceso que dichas empresas deben cumplir. En suma, si los datos de los colombianos salen fuera del territorio colombiano, se expone a los ciudadanos a riesgos jurídicos y políticos surgidos de las regulaciones de los otros países o de las decisiones de autoridades y gobiernos extranjeros.

Este año por ejemplo, el gobierno norteamericano, adoptó una decisión soberana que prácticamente dice que los datos de los colombianos que reposen en data centers, bancos de datos o archivos ubicados en ese país quedarán sin protección, o por lo menos serán excluidos, de las políticas de privacidad de las agencias de seguridad de los Estados Unidos.

A continuación trascribimos la parte pertinente de la reciente orden ejecutiva sobre el tema:

> **"*The White House***
> *Office of the Press Secretary*
> *For Immediate Release*
> *January 25, 2017*
> *Executive Order: Enhancing Public Safety in the Interior of the United States*
>
> *EXECUTIVE ORDER*
>
> *(…)*
>
> *ENHANCING PUBLIC SAFETY IN THE INTERIOR OF THE UNITED STATES*

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Immigration and Nationality Act (INA) (8 U.S.C. 1101 et seq.), and in order to ensure the public safety of the American people in communities across the United States as well as to ensure that our Nation's immigration laws are faithfully executed, I hereby declare the policy of the executive branch to be, and order, as follows:

Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[18]

Frente a esta situación nace la siguiente pregunta: **¿Deben los colombianos asumir los riesgos jurídicos, políticos y soberanos de otros países que emergen con ocasión de la decisión de un empresario de exportar datos personales desde Colombia a esos países?**.

d) Desconocimiento por parte de algunas empresas extranjeras de las leyes y de la competencia de las autoridades locales de protección de datos

Debe tenerse presente que ciertas empresas extranjeras alegan ante las autoridades locales de protección de datos que ellas no son competentes para investigarlas y que la ley local no les aplica. Así por ejemplo, es mundialmente conocido el caso de Google Inc (domiciliado en el Estado de California de los Estados Unidos) y la Agencia Española de protección de datos.

[18] Tomado de: https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united . Una traducción no oficial de la sección 14 es la siguiente:
"14. Ley de Privacidad. Las agencias se asegurarán de que sus políticas de privacidad excluyan a las personas que no sean ciudadanos de los Estados Unidos o residentes permanentes legales de las protecciones de la Ley de Privacidad en lo que respecta a la información de identificación personal."

En efecto, en la resolución R/02892/2013 de dicha Agencia se constata lo anterior, en los siguientes términos: *"3.- Google Inc., y los tratamientos de datos personales que realiza, no entran dentro del ámbito territorial de aplicación de la LOPD.* ***Google rechaza rotundamente que esté sujeto a los requisitos de protección de datos de la legislación española****, excepto para aquellos casos concretos en que ha notificado operaciones de tratamiento de datos a la Agencia (StreetView). Como entidad estadounidense, utiliza medios para el tratamiento de datos que no están localizados dentro de la jurisdicción española y, por tanto, no entra dentro de los criterios de aplicación territorial que preceptúa el artículo 2.1.c) de la LOPD"*[19] (Destacamos)

Esta doctrina corporativa evidencia, en cierta medida, el nivel de interés que tienen algunas empresas extranjeras por respetar las leyes locales de otros países. Estas empresas solo respetan la ley de la oferta y la demanda y su ley corporativa, es decir las normas unilaterales que redactan para proteger su modelo de negocio. Todo lo anterior, per se, no es incorrecto siempre y cuando no se abuse del poder informático para desconocer o disminuir la efectividad de los derechos de los titulares de los datos.

e) Imposición de cargas adicionales a los colombianos para el ejercicio de sus derechos.

El ciudadano colombiano cuyos datos estén en una empresa no domiciliada en Colombia tendrá que someterse a las políticas internas de esa empresa para ejercer sus derechos. Así las cosas, no regirán los procesos y términos que establecen los artículos 14 y 15 de la ley 1581 de 2012 sino las estipulaciones

[19] Cfr. Agencia Española de Protección de Datos. Procedimiento No PS/00345/2013 RESOLUCIÓN: R/02892/2013. Procedimiento sancionador PS/00345/2013, instruido por la Agencia Española de Protección de Datos a las entidades GOOGLE INC. y GOOGLE SPAIN, S.L. El texto completo de la resolución puede consultarse en: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/AEPD-13-resolucionSancion-Google1.pdf

contractuales que unilateralmente establecen las empresas mediante contratos de adhesión. Esto es lo que se ha denominado como el ***"Internet of Corporations"*** -*IoC*- o el "**Internet de las empresas**"[20].

En este punto debemos preguntarnos lo siguiente: **¿las empresas extranjeras no domiciliadas en Colombia deben someterse a las leyes colombianas o el Estado colombiano y los (as) colombianos (as) debe someterse a las políticas de esas empresas extranjeras?.**

A lo anterior se suma todo lo mencionado en los aspectos citados previamente como: (i) Inaplicabilidad de la ley colombiana, sometimiento de los colombianos a leyes y jueces extranjeros y no garantía plena del habeas data; (ii) pérdida de control de la información; (iii) Sometimiento de los colombianos a las decisiones de las autoridades o gobiernos de otros países; (iv) Desconocimiento por parte de algunas empresas extranjeras de las leyes locales y la competencia de las autoridades locales de protección de datos, lo cual afecta la plena garantía del habeas data.

Visto lo anterior, a continuación presentamos nuestras solicitudes y sugerencias

5. **Solicitudes y sugerencias sobre el proyecto de circular**.

5.1. Permitir la libre circulación transfronteriza de datos públicos sobre comerciantes y empresarios

[20] Sobre este tema ver: *"Internet de las empresas" ["Internet of Corporations" -IoC-]: Una explicación de lo que pasa en internet y del futuro de la protección de los derechos humanos en el ciberespacio (Parte 1)*. Publicado en: https://habeasdatacolombia.uniandes.edu.co/?p=2222

Sugerimos adicionar el siguiente párrafo al numeral 3.2. del proyecto de circular:

> *"Parágrafo 2: La transferencia y la transmisión internacional de datos personales públicos sobre comerciantes y empresarios será libre y no requerirá cumplir ningún requisito legal para la circulación transfronteriza de los mismos*."

Varias razones motivan nuestra solicitud, a saber:

- El tratamiento de datos personales públicos no requiere de la autorización del titular del dato por mandato expreso del literal b) del artículo 10 de la ley 1581 de 2012.

- La información que reposa en las Cámaras de Comercio es pública y por ende no es necesario obtener el consentimiento de los titulares de los datos para tratarla. En efecto, el Registro Mercantil es público y que "*cualquier persona podrá examinar los libros y archivos en que fuere llevado, tomar anotaciones de sus asientos o actos y obtener copia de los mismos*"[21] . Este derecho aplica a cualquier persona con independencia de su nacionalidad, residencia o domicilio.

- El tratamiento de datos personales implica cualquier actividad u operación sobre dicha información, tal y como lo establece el literal g) del artículo 3 de la ley 1581 de 2012.

- La Corte Constitucional ha establecido que "*la información pública es aquella que "puede ser obtenida y ofrecida sin reserva alguna y sin importar*

[21] Cfr. Artículo 26 del Código de Comercio

si la misma sea información general, privada o personal". Es decir la información *"que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno*"[22]. Recalca la Corte que "*la información pública, en tanto* no *está relacionada con el ámbito de protección del derecho a la intimidad, recae dentro del ejercicio amplio del derecho a recibir información (Art. 20 C.P.) y, en consecuencia, es de libre acceso*"[23].

- Según el artículo 3 del decreto 1377 de 2013, son datos personales de carácter público, entre otros, "*los datos relativos al estado civil de las personas,* ***a su profesión u oficio*** *y* ***a su calidad de comerciante*** *o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva*" (Destacamos). De otra parte, el artículo 5 del citado decreto establece que "*Los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o bases de datos que se encuentren a disposición del público,* ***pueden ser tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos****.".*

- Como se observa, los datos relacionados con la actividad mercantil de personas naturales pueden ser tratados por cualquier individuo en Colombia o fuera del país. Adicionalmente, **el párrafo segundo del literal f) del artículo 4 de la ley 1581 de 2012 permite que los datos públicos se divulguen en internet o en otros medios de comunicación masiva**[24].

[22] Cfr. Corte Constitucional, sentencias T-729 de 2002; C-336 de 2007, C-1011 de 2008, C-334 de 2010

[24] El párrafo segundo del literal f) del artículo 4 de la ley 1581 de 2012 dice lo siguiente: "*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*;"

- Internet, por su naturaleza, es una herramienta de tratamiento de datos y de comunicación a escala global y transfronteriza.

- La ley estatutaria 1581 de 2012 debe aplicarse en concordancia con otra ley estatutaria posterior y especial sobre los datos públicos como lo es la ley 1712[25] de 2014.

- El principio de máxima publicidad previsto en el artículo 2[26] de la ley 1712 es la principal pauta a seguir tratándose de datos públicos. Esa máxima publicidad es consistente con la libre circulación nacional e internacional de dicha información.

- El principio de transparencia obliga a los responsables del tratamiento de datos públicos a "*proporcionar y facilitar el acceso a la misma en los términos más amplios posibles*"[27]. En este sentido la libre circulación de datos personales públicos es consistente con el deber de facilitar el acceso a información pública de manera abierta y amplia a todos los sujetos que requieran de ella.

- El anterior mandato legal también debe aplicarse de manera armónica con el "principio de la divulgación proactiva de la información" según el cual existe el deber de "*promover y generar una cultura de transparencia, lo que conlleva la obligación de publicar y divulgar documentos y archivos que plasman la actividad estatal y de interés público, de forma rutinaria y proactiva, actualizada, accesible y comprensible*" [28].

[25] Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
[26] "*Artículo 2°. Principio de máxima publicidad para titular universal. Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley*." (Ley 1712 de 2014)
[27] Cfr. Artículo 3 de la ley 1712 de 2014
[28] Cfr. Artículo 3 de la ley 1712 de 2014

La información pública sobre los comerciantes (personas jurídicas o naturales) es de interés público porque existe un interés legítimo de otros empresarios, los consumidores y la sociedad en general de conocer información sobre las empresas con las que van a realizar negocios con miras a mitigar cualquier riesgo jurídico de eventual fraude o estafa. En últimas el libre acceso y circulación a información pública de los empresarios contribuye a tomar decisiones informadas y evitar engaños a la sociedad en general y los consumidores en especial.

Cualquier empresa nacional o extranjera que desee entablar relaciones comerciales con otra tiene el interés legítimo de conocer, por lo menos, toda la información pública sobre la parte con que hará negocios. Esto es algo básico que forma parte del "*due diligence*" en los negocios.

- La economía digital requiere del flujo libre de datos públicos sobre empresarios. La actividad mercantil es cada vez más transfronteriza, global y tecnológica. Por esta razón, la información pública sobre comerciantes de un país es de mucho interés de los comerciantes y consumidores de otros países que deseen realizar negocios con los empresarios de otros países.

La no circulación libre y transfronteriza de datos personales sobre los comerciantes podría facilitar actividades fraudulentas, engañosas y delictuales.

- El interés legítimo que tiene la sociedad, los empresarios y los consumidores (nacionales o extranjeros) de conocer la información pública sobre los comerciantes ha sido el principal motivo por el cual el tratamiento de datos sobre ellos es excluido de las normas de tratamiento de datos personales. Este es el caso, por ejemplo, de España.

En efecto, esto ordena el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[29]:

"*Artículo 2 Ámbito objetivo de aplicación*

(…)

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ***ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales****.*

3. Asimismo, ***los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal****.*

(…) " (Destacamos)

Obsérvese como el interés legítimo sobre el conocimiento de información pública de los comerciantes justifica el libre tratamiento y circulación nacional e internacional de esa información.

[29] El texto del Real Decreto puede consultarse en: http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.t1.html#a2

5.2. Exigir la verificación de la efectividad de los medios administrativos o judiciales para la protección de los derechos de los colombianos cuando sus datos están en bases de datos o archivos ubicados en otros países como consecuencia de una transferencia internacional

El literal e) del numeral del proyecto de circular dice lo siguiente:

"3.1 Estándares de un nivel adecuado de protección en el país receptor de la información personal
(...)

e) 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."
Sugerencia:

Recomendamos que en la circular explícitamente se exija que:
(1) esos mecanismos de los otros países también apliquen o beneficien a titulares de datos extranjeros y no domiciliados en ese país, y
(2) se pueda hacer ejercicio de los mecanismos mediante herramientas tecnológicas gratuitas que no impliquen desplazamientos ni costos que impidan o anulen las posibilidades de real protección de los derechos del titular del dato colombiano cuyos datos fueron transferidos a otro país.

Nuestra observación tiene origen en el hecho de que en algunos países o estados la nacionalidad es un requisito para que una persona pueda acudir a las autoridades administrativas o judiciales.

Es necesario que la SIC se asegure que cuando se transfirieran los datos a otro país no mueran o desaparezcan los derechos y las garantías que tanto la ley 1581 de 2012 como la SIC ofrecen y garantizan a los titulares de los datos en Colombia.

En fin, las garantías y los procesos en otro países no deben ser *"letra muerta",* sino herramientas sencillas, gratuitas y efectivas como lo son en Colombia. Los titulares de los datos no deben ser afectados por la decisión de Responsable de exportar los datos a otro país.

5.3. Necesidad de suscribir un contrato de transferencia internacional de datos para garantizar los derechos de los titulares de los datos cuya información es transferida a otro país.

El parágrafo del numeral 3.2. del proyecto de circular dice lo siguiente:

"3.2 Países que cuentan con un nivel adecuado de protección de datos personales
(...)
Parágrafo: Cuando la Transferencia de datos personales se vaya a realizar a un país que no se encuentre en el listado presentado en este numeral, corresponderá al Responsable del tratamiento que realizará la transferencia verificar si ese país cumple con los estándares fijados en el numeral 3.1 anterior, caso en el cual podrá realizar la trasferencia, o, de no cumplirlos, solicitar la respectiva declaración de conformidad ante esta Superintendencia."

El texto réplica la idea consagrada en la parte segunda del literal f) del artículo 5 de la ley 1266 de 2008, que dice lo siguiente:

"Artículo 5°. *Circulación de información*. La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los 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) (...) Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo 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." (Esta norma esta derogada por la ley 1581 de 2012.)

La propuesta de la circular deja en manos del responsable exportador de los datos todo lo atinente a la transferencia internacional de información sin ningún

control previo estatal, ni consagrar alguna herramienta o garantía de los derechos de los titulares de los datos personales.

El principal interés del responsable es exportar los datos, mientras que la SIC tiene la función legal de ejercer la "vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley" y "a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;" (Artículos 19 y 21 de la ley 1581 de 2012)

Creemos que con la circular se abren puertas para facilitar la transferencia internacional, pero al mismo tiempo se cierran las puertas para que se respeten y protejan efectivamente los derechos de los titulares de los datos transferidos.

Así las cosas, y con miras a llegar a un punto intermedio, sugerimos lo siguiente:

Que se exija la firma de un contrato de transferencia internacional en el cual se establezca lo siguiente:

a) Que el responsable exportador de los datos continúa siendo responsable de los derechos de los titulares de los datos transferidos.
b) Que el ejercicio de los derechos de los titulares de los datos se realice ante el responsable exportador de los datos quien hará todo lo necesario para que el responsable importador o receptor garantice los derechos del titular. En caso de no ser así, el responsable exportador será multado en Colombia por la SIC y responderá de los daños y perjuicios causados al titular.
c) Que el responsable exportador y el responsable importador sean solidariamente responsables ante la autoridad colombiana y el titular del dato por el eventual incumplimiento de la ley 1581 de 2012, sus decretos reglamentarios y demás instrucciones que emita la SIC.

En suma, está propuesta busca que se suscriba un contrato similar al que se exige para las transmisiones internacionales pero con mayores exigencias porque en la transferencia el responsable de tratamiento deja de ser responsable del mismo, cuestión que no sucede en la transmisión.

En adición a lo anterior, el contrato de transferencia internacional de datos deberá incluir lo siguiente:

- **Nombre, finalidad y tipo de tratamiento de la base de datos** del responsable exportador que contiene la información personal objeto de la transferencia internacional

- **Obligaciones del exportador de datos**. Por ejemplo exigir las siguientes: a) Asegurar que la recopilación, el tratamiento y la transferencia de los datos personales se han efectuado de conformidad con la legislación colombiana.; b) Realizar esfuerzos razonables para determinar si el importador de datos es capaz de cumplir las obligaciones jurídicas que le incumben en virtud de las presentes cláusulas y de la ley 1581 de 2012.; c) Responder en el término establecido en la ley 1581 de 2012 las consultas o reclamos que presenten los titulares de los datos tanto al exportador como el importador de los datos. Cuando la consulta o reclamos se presente al importador, este la trasladará inmediatamente al exportador para que responda oportunamente al titular del dato.

- **Obligaciones del importador o receptor de los datos**. Incluir las siguientes, por lo menos, las siguientes: a) Implementar las medidas técnicas y organizativas que resulten necesarias para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración accidentales o su divulgación o acceso no autorizados, y que garanticen el nivel de seguridad apropiado a los riesgos que entraña el tratamiento y a la naturaleza de los datos que han de protegerse; b) Disponer de procedimientos que garanticen que cualquier tercero al que dé acceso a los datos *personales*, incluidos los encargados del tratamiento, respetarán y preservarán la confidencialidad y seguridad de los datos personales. c) Tratar los datos personales de conformidad con la ley 1581 de 2012 de la República de Colombia y sus decretos reglamentarios para los siguientes fines: …….. d) Comunicar al exportador de datos un punto de contacto dentro de su organización autorizado para responder a las consultas que guarden relación con el tratamiento de datos personales y cooperará de buena fe con el exportador de datos, el titular de los datos y la autoridad de protección de datos respecto de tales consultas dentro del período permitido por la ley colombiana. e) Poner a disposición del exportador de datos, a petición de éste, sus instalaciones de tratamiento de datos, sus archivos y toda la documentación necesaria para el tratamiento,

a efectos de revisión, auditoría o certificación. Estas labores serán realizadas, previa notificación razonable y durante horas laborables normales, por el exportador de datos (o por un inspector o auditor imparcial e independiente por él designado y al que no se haya opuesto razonablemente el importador de datos) a fin de determinar si se cumplen las garantías y los compromisos previstos en las presentes cláusulas.

- **Responsabilidad y derechos de terceros.** Establecer, por ejemplo, lo siguiente: Cada una de las partes deberá responder ante los titulares de los datos por los daños que le hubiese provocado como resultado de la eventual vulneración de sus derechos. Ello no afecta a la responsabilidad del exportador de datos con arreglo a la legislación colombiana.

- **Garantías respecto de la protección de los datos personales objeto de tratamiento.** Incluir, por lo menos, lo siguiente: a) Los titulares de los datos podrán presentar frente al EXPORTADOR o el IMPORTADOR DE DATOS las consultas y reclamos a que se refieren los artículos 14 y 15 de la ley 1581 de 2012; b) Las consultas y reclamos serán tramitadas y respondidas dentro de los plazos establecidos en precitados artículos de la ley 1581 de 2012; c) La atención debida y oportuna de las consultas y reclamos será responsabilidad del EXPORTADOR DE DATOS. Para el efecto, el IMPORTADOR DE DATOS informará inmediatamente al EXPORTADOR DE DATOS sobre cualquier consulta o reclamo que le sea presentado por el titular del dato o cualquier persona legitimada a la luz de la regulación colombiana; d) El IMPORTADOR DE DATOS se compromete a garantizar al titular del dato los derechos que tiene a la luz de la regulación colombiana. El EXPORTADOR DE DATOS realizará todas las acciones necesarias para hacer valer los derechos de los titulares de los datos; e) El IMPORTADOR DE DATOS se compromete a cumplir los deberes que le impone el artículo 17 de la ley 1581 de 2012, salvo realizar el registro de base de datos ante la SIC.

- **Mecanismos o canales implementados por el importador o destinatario de la transferencia para la atención de consultas, peticiones y reclamos de los titulares de los datos**.

- **Medidas de seguridad y confidencialidad previstas para realizar la transferencia internacional de datos y para proteger los datos cuando se almacenen en equipos o data centers ubicados fuera del territorio colombiano**

- **Resolución de conflictos con los titulares de los datos o con las autoridades de protección de datos**. Incluir lo siguiente: a) En caso de conflicto o de reclamación interpuesta contra una o ambas partes del contrato de transferencia por un titular del dato o por la autoridad en relación con el tratamiento de datos personales, la una informará a la otra sobre esta circunstancia y ambas cooperarán con objeto de alcanzar una solución dentro de los términos permitidos por la regulación colombiana; b) Las partes acuerdan responder a cualquier procedimiento que haya sido iniciado por un titular del dato o por la autoridad de protección de datos; c) Cada una de las partes se compromete a acatar cualquier decisión de la autoridad de protección de datos o los tribunales competentes de la República de Colombia.

- **Suspensión de la transferencia y terminación del contrato.** Incluir lo siguiente: a) En caso de que el IMPORTADOR DE DATOS incumpla las obligaciones que le incumben en virtud de las presentes cláusulas, el EXPORTADOR DE DATOS deberá suspender temporalmente la transferencia de datos personales al importador hasta que se subsane el incumplimiento o se resuelva el contrato; b) El EXPORTADOR DE DATOS, sin perjuicio del ejercicio de cualquier otro derecho que le pueda asistir contra el IMPORTADOR DE DATOS, podrá terminar el presente contrato en caso de que:(i) la transferencia de datos personales al importador de datos haya sido suspendida temporalmente por el exportador de datos durante un período de tiempo superior a tres meses;(ii) el incumplimiento por parte del importador de datos del contrato de transferencia internacional de datos; (iii) el importador de datos incumpla de forma sustancial o persistente cualquier garantía o compromiso previstos en las presentes cláusulas; (iv) una decisión final contra la que no pueda entablarse recurso alguno de un tribunal competente del país de establecimiento del exportador de datos o de la autoridad establezca que el importador o el exportador de datos han incumplido las cláusulas;

- **Legislación aplicable.** Es imprescindible que el contrato se rija por la legislación de la República de Colombia, especialmente la ley 1581 de 2012 y sus normas reglamentarias.

Finalmente, sugerimos consultar los modelos de cláusulas contractuales como, entre otros, los siguientes:

- VERSIÓN CONSOLIDADA de la Decisión 2001/497/CE, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país (***Transferencias internacionales entre responsables del tratamiento***) Disponible en: https://habeasdatacolombia.uniandes.edu.co/?page_id=2000

5.4. Analizar si la ley 1581 de 2012 faculta a SIC para emitir declaraciones de conformidad de transmisiones internacionales de datos.

Según la parte iii) del literal b) del numeral 3.3. *-Transmisión Internacional de Información Personal-* la SIC puede proferir declaración de conformidad de las transmisiones internacionales.

El literal g) del artículo 21 de la ley 1581 de 2012 dice lo siguiente:

"Artículo 21. *Funciones*. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:
(...)
g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos; (...)" (Subrayo)

La ley estatutaria no le otorga a la SIC la función de proferir declaraciones de conformidad para las transmisiones internacionales de datos. Por lo anterior, respetuosamente se solicita a la SIC reflexionar sobre este tema.

Reiteramos nuestra gratitud por leer y analizar estas sugerencias que escribimos pensando en lo mejor para Colombia y los titulares de los datos personales que se tratan en nuestro país.

Cordialmente,

NELSON REMOLINA ANGARITA

Profesor Asociado. Director del GECTI y del Observatorio CIRO ANGARITA BARÓN sobre la protección de datos personales en Colombia.