

Bogotá D.C., 08 de Marzo de 2017

Doctor  
**PABLO FELIPE ROBLEDO**  
Superintendente  
**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**  
La Ciudad

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 17-059141- -00000-0000

Fecha: 2017-03-08 15:31:29 Dep. 12 GRUPOREGULAC  
Tra. 334 REMISIINFORMA Eve:  
Act. 411 PRESENTACION Folios: 13

JB 1

**Asunto: Comentarios al proyecto de circular única por la cual se pretende "Adicionar un Capítulo Tercero al Título V de la Circular Única"**

Apreciado doctor Robledo,

Desde la Cámara Colombiana de Informática y Telecomunicaciones – CCIT, reconocemos la importante labor que está desarrollando la Superintendencia de Industria y Comercio, en aras de reforzar la seguridad y protección de los datos personales de los colombianos.

En virtud de lo anterior, y atendiendo a la amable invitación que se hace para presentar comentarios al proyecto de Circular Única por la cual se pretende "Adicionar un Capítulo Tercero al Título V de la Circular Única", nos permitimos presentar los siguientes:

#### **I. Comentarios generales al proyecto de circular**

El uso de servicios tecnológicos, que implican el movimiento transfronterizo de información como el *cloud computing*, el comercio móvil y el Internet de las Cosas, ha permitido entre otros, la aparición de una nueva eficiencia global y nuevo un mercado mundial. Por ello, y con el fin de aprovechar el potencial de la economía digital, es necesario que cada uno de los países adopte un marco de políticas públicas que fomenten la inversión de las tecnologías e innovación para las generaciones venideras.

En este orden de ideas, y con el fin de minimizar los impactos que puedan tener para los negocios de las empresas el cambio de regulación, limitar la transferencia de datos tendrá una consecuencia negativa para el sector, toda vez que la naturaleza de su negocio jurídico radica en el intercambio de información.

Igualmente, es importante que se tenga en cuenta los compromisos adquiridos por Colombia y los Estados Unidos en el TLC dentro del cual se estableció que los empresarios provenientes de los Estados Unidos han realizado inversiones a largo

2

plazo, con el fin de incrementar su capacidad productiva y con ello la conservación de las condiciones igualitarias para el desarrollo de sus negocios. Dentro del capítulo 14 de telecomunicaciones, en su artículo 14.2 numeral 3 que *“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 las Partes.”*

Por ello, consideramos que las propuestas regulatorias que se expidan deberían velar por promover la interoperabilidad de las normas de protección de datos personales, y con ello hacer los procesos administrativos automatizados y seguros.

Así pues, es importante que esta Superintendencia tenga presente algunos de los siguientes puntos, dentro de la expedición de su normativa, con el fin de promover el desarrollo de las tecnologías de la información y las comunicaciones, tales como: i) **Protección de los consumidores**: Respaldar las leyes de protección de datos de los consumidores relacionadas con las actividades comerciales fraudulentas y engañosas en línea y con ello asegurar que tanto su privacidad como otros derechos; ii) **Habilitación del flujo transfronterizo de datos**: Asegurar el libre flujo de información a través del cual se garantice que dicho procedimiento contará con la protección de información personal adecuada para los colombianos; iii) **Promoción de la interoperabilidad**: Fomentar la creación de políticas públicas encaminadas a la cooperación regulatoria con otros países con los que exista o se requiera un amplio flujo transfronterizo de datos.

Por ello, respetuosamente sugerimos que se cree un sistema que permita la flexibilidad e interoperabilidad entre países, sobre transferencias de datos personales, como sucede en el caso del GDPR<sup>1</sup> y el APEC<sup>2</sup>; y facilitara la transferencia de datos. En estos sistemas las partes, en ejercicio de la autonomía de la voluntad, pueden implementar medidas contractuales que les permitirá garantizar la protección de los datos personales de los colombianos, ampliando o siguiendo las ya contempladas en la Ley 1581 de 2012 y el Decreto 1377 de 2013, incorporado en el Decreto 1074 de 2015, sin que implique un desgaste administrativo para cada una de las partes involucradas.

## **II. Comentarios específicos al proyecto de circular**

### **Comentarios al numeral 3.1 del proyecto de circular**

<sup>1</sup> The General Data Protection Regulation (GDPR – EU 2016/679)

<sup>2</sup> APEC Privacy Framework

### ***“3.1. Estándares de un nivel adecuado de protección en el país receptor de la información personal***

*El análisis para establecer si un país ofrece un nivel adecuado de protección de datos personales, a efectos de realizar una transferencia internacional de datos, estará orientado a determinar si dicho país garantiza la protección de los mismos, con base en los siguientes estándares:*

- a) Existencia de normas aplicables al tratamiento de datos personales.*
- b) 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.*
- c) Consagración normativa de derechos de los Titulares.*
- d) Consagración normativa de deberes de los Responsables y Encargados.*
- e) Existencia de medios y vías jurídicas y/o administrativas para garantizar la tutela de los derechos de los Titulares y exigir el cumplimiento de la Ley.*
- f) 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.”*

Según lo establecido por la jurisprudencia de la Corte Constitucional, en Sentencia C – 748 de 2011 *“un país cuenta con los elementos o estándares de garantía necesarios para garantizar un nivel adecuado de protección de datos personales, si su legislación cuenta con unos principios, que abarquen las obligaciones y derechos de las partes (titular del dato, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos de datos personales), y de los datos (calidad del dato, seguridad técnica) y; con un procedimiento de protección de datos que involucren mecanismos y autoridades que efectivicen la protección de la información”.*

En línea con lo anterior, y con lo establecido por la Corte Constitucional, respetuosamente sugerimos que los estándares establecidos dentro del proyecto objeto de estudio se establezcan de la siguiente manera, en esta nueva redacción de texto propuesta.

### ***“3.1. Estándares de un nivel adecuado de protección en el país receptor de la información personal***

*El análisis para establecer si un país ofrece un nivel adecuado de protección de datos personales, a efectos de realizar una transferencia internacional de datos, estará*

4

orientado a determinar si dicho país garantiza la protección de los mismos, con base en los siguientes estándares:

- a) Existencia de normas aplicables al tratamiento de datos personales.
- b) ~~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.~~
- c) Consagración normativa de derechos de los Titulares.
- d) **Consagración normativa de los deberes de quienes realicen Tratamiento de Datos.**
- e) **Existencia de procedimientos para garantizar la protección de la información, los cuales podrán ser de carácter: administrativo, judicial, extrajudicial o privado.**
- f) **Existencia de autoridad (es) encargada (s) de la protección de datos personales o de privacidad"**
- g) ~~Consagración normativa de deberes de los Responsables y Encargados.~~
- h) ~~Existencia de medios y vías jurídicas y/o administrativas para garantizar la tutela de los derechos de los Titulares y exigir el cumplimiento de la Ley.~~

~~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."~~

### **Comentarios al numeral 3.2. del proyecto de circular**

#### **"3.2. Países que cuentan con nivel adecuado de protección de datos personales.**

Teniendo en cuenta los estándares señalados en el numeral 3.1 anterior, a continuación se relacionan los países que garantizan un nivel adecuado de protección:

- a) Albania
- b) Alemania

(...)

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 transferencia, o, de no cumplirlos, solicitar la respectiva declaración de conformidad ante la Superintendencia."

Al respecto, no se tiene certeza sobre el mecanismo usado por parte de la Superintendencia en relación con la definición del listado de países que a su consideración cuentan con los estándares necesarios para una adecuada transmisión de datos. Sin embargo, vemos con preocupación que países como Estados Unidos y Brasil, no se encuentran incluidos dentro de esta lista; así como tampoco lo están Aruba, Bahamas, Chile, Curazao, Ecuador, República Dominicana, Nicaragua y Trinidad y Tobago. Por ejemplo en el caso de Brasil, se hizo la siguiente revisión en relación con los estándares incluidos por esta Superintendencia, con el fin de poder determinar si cuenta con los niveles adecuados de protección de datos personales, como se explica a continuación:

**“I. Mecanismos Brasileños de Protección de Datos**

**A) Existencia de normas aplicables al tratamiento de datos personales.**

*Aunque Brasil no cuenta con un único estatuto de Protección de Datos Personales, si cuenta con un Código del Consumidor (número 8,078/90) y una Ley Federal de Internet (número 12.695/2014), y con un Decreto Regulatorio No. 8.771/16 del 11 de mayo de 2016, los cuales incluyen algunas disposiciones sobre seguridad y tratamiento de datos personales.*

**B) 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.**

*La Ley Brasileira de Internet establece como fundamentos: la libertad de expresión, los derechos humanos, la pluralidad y colaboración. A su vez, incluye principios como la protección a la privacidad y preservación de la seguridad.*

**C) Consagración normativa de los derechos del titular de los derechos de protección de datos personales.**

*Con respecto a los derechos de los usuarios, la Ley Brasileira de internet establece específicamente los siguientes derechos:*

- *Inviolabilidad de la vida privada;*
- *Inviolabilidad de las comunicaciones, salvo orden judicial;*
- *Información correcta y clara de los contratos de prestación de servicios;*
- *Los datos personales no podrán ser proporcionados a terceros sin el consentimiento del usuario.*
- *Aplicación de los derechos de protección al consumidor a las relaciones a través de internet.*
- *El Código del Consumidor establece puntualmente los siguientes derecho en su Sección VI, Art. 43:*

- *Derecho del consumidor al acceso sobre las informaciones existentes en registros y bases de datos y puntualmente sobre los datos personales que sobre el existan así como sus respectivas fuentes;*
- *Derecho a que se le informe de manera previa sobre la apertura de un registro o base de datos personales;*
- *Derecho a que se corrija cualquier información incorrecta que sobre él exista;*

**D) Consagración normativa de los deberes de Responsables y Encargados de los datos personales.**

*En general, se requiere que los procesadores de datos en Brasil tomen medidas razonables técnicas, físicas y organizacionales para proteger la seguridad de los datos personales. Sin embargo, no existen requerimientos específicos, restricciones o detalles en cómo debe ser implementada la seguridad.*

*El Decreto de Ley Brasileira de Internet establece que los proveedores de servicios, y proveedores de redes y aplicaciones deben mantener confidenciales los registros de acceso (tales como direcciones IP, inicios de sesión, etc.) de los usuarios, en un ambiente seguro y controlado, acorde a los siguientes estándares de seguridad:*

- *Control estricto al acceso de datos definiendo quien tendrá acceso y privilegios de acceso exclusivo a ciertos usuarios.*
- *Mecanismos de autenticación para control de accesos usando, por ejemplo, sistemas de doble autenticación para asegurar la individualización de registros.*
- *Creación de control un inventario detallado del acceso a la conexión y registros de acceso a las aplicaciones, los cuales deben contener tiempo, duración, identificación del empleado o persona responsable y los archivos a los que accedió.*
- *Usar soluciones de administración de registros que aseguren tanto la inviolabilidad de los datos, como la encriptación o las medidas de protección equivalentes.*

**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.**

*Si bien no existe sanción específica por no cumplir con las garantías definidas en el Decreto Regulatorio de la Ley Brasileira de Internet, la aplicación de la Ley se puede exigir a través de:*

- *Procesos Administrativos*
- *Demandas civiles individuales, o*
- *Acciones colectivas*

*Estas medidas pueden ser iniciadas por:*

- *El titular de los datos.*
- *Autoridades públicas (ej. La Fiscalía, la Oficina de Protección al Consumidor y el regulador para la respectiva industria), o*
- *Por asociaciones que defiendan intereses colectivos.*

7

Dichas autoridades públicas podrán imponer multas y, cuando sea relevante, revocar licencias o permisos. Los daños civiles pueden ser significativos, pues las violaciones al derecho a la privacidad pueden dar derecho al demandante a indemnización por daños morales.

Vale la pena mencionar que la Ley Brasileira de Internet también establece que las violaciones a los derechos a la privacidad y/o intimidad en internet están sujetas a una multa de hasta el 10% (diez por ciento) del valor total de la facturación del grupo económico de la empresa en el país. Las oficinas o subsidiarias de empresas extranjeras establecidas en Brasil son responsables solidariamente del pago de las multas.

Por otro lado, el Código al Consumidor establece en si Título II, Artículos 72 y 73 sanciones que pueden ser la detención o multa en caso que (i) se impida o dificulte el acceso al consumidor sobre las informaciones que conste en registros, bancos de datos y ficha o (ii) no se corrija inmediatamente información que conste en registros o bases de datos que se sepa o se deba saber es inexacta.

**F) 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.**

Para la supervisión del tratamiento de datos personales, el Decreto mencionado anteriormente incluye los responsables de los siguientes temas:

- La Agencia Nacional de Telecomunicaciones actuará en la regulación, inspección y verificación de infracciones relacionadas con servicios de telecomunicaciones;
- La Secretaría Nacional del Consumidor actuará en la inspección relacionada a los derechos del consumidor;
- El Sistema Brasileiro de Defensa de la Competencia inspeccionará las infracciones de orden económico;
- Otras entidades de la administración federal actuarán de manera colaborativa acorde a sus competencias respecto a los asuntos planteados por el decreto.

**G) Acceso a la Legislación Referenciada.**

Ley Brasileira de Internet - [http://www.planalto.gov.br/ccivil\\_03/ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm)

**Código del Consumidor – [http://www.planalto.gov.br/ccivil\\_03/leis/L8078.htm](http://www.planalto.gov.br/ccivil_03/leis/L8078.htm)**

**II. Mecanismos de protección de datos usados en los Estado Unidos**

**a) Existencia de normas aplicables al tratamiento de datos personales.**

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 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 vídeo). Muchos Estados también contaban con leyes análogas en estos ámbitos<sup>3</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 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*

<sup>3</sup> Apéndice A 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.



las Cartas de Seguridad Nacional, una forma de citaciones administrativas autorizadas por ley (6)<sup>4</sup>.

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

**b) 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 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, 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

<sup>4</sup> Carta del Asesor General, Robert Litt, Director de la Oficina del Director de Inteligencia Nacional al Departamento de Comercio de EE.UU.

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”.

**c) 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”.

**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.**

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”.

**f) 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.”

Así pues, y entendiendo que estos países cuentan y cumplen con los mejores estándares en protección de datos personales, respetuosamente solicitamos que

los mismos sean incluidos dentro de la citada norma, toda vez que gran mayoría de las empresas cuentan con su infraestructura y prestación de servicios en los mismo, y al no incluirse se podría generar en consecuencia una incertidumbre jurídica.

Adicional a esto, no es claro en qué momento se entiende que las empresas han cumplido con los estándares fijados dentro del proyecto, ni cual es el procedimiento usado por esta Superintendencia para otorgar la autorización al país que cumpla los requisitos, así como tampoco la forma en la que se llevará a cabo la actualización de lista por parte de la autoridad, bien sea para incluir o eliminar países. Lo anterior, genera incertidumbre ya que en la medida en la que no se establezca como se llevará a cabo este procedimiento de autodeterminación por parte de las compañías, la Superintendencia podrá emitir sanciones, lo que en consecuencia aumentará el número de solicitudes de declaraciones de conformidad para así evitar incurrir en estas. Razón por la cual, respetuosamente solicitamos se aclare el mismo.

Finalmente, no es clara la norma en establecer el procedimiento a través del cual se deberá solicitar la declaración de conformidad, tramitada y expedida por la misma Superintendencia, cuando se realice transferencia de datos con países que no se encuentren incluidos de manera taxativa dentro de la norma. En razón de ello, respetuosamente solicitamos que se haga la debida aclaración, así como el plazo de implementación de exigibilidad de la Circular objeto de estudio.

En virtud de lo anterior, ponemos a consideración la siguiente redacción de texto:

***"3.2. Países que cuentan con nivel adecuado de protección de datos personales.***

*Teniendo en cuenta los estándares señalados en el numeral 3.1 anterior, a continuación se relacionan los países que garantizan un nivel adecuado de protección:*

- c) Albania
- d) Alemania
- e) Aruba
- f) (...)
- g) Brasil
- h) Bahamas
- i) Chile
- j) Curazao
- k) Ecuador
- l) (...)
- m) Estados Unidos
- n) Trinidad y Tobago
- o) República Dominicana
- p) Nicaragua

13

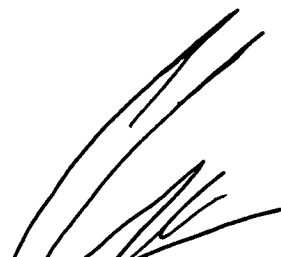
(...)"

Esperamos haber contribuido de manera positiva con nuestros aportes, los cuales respetuosamente solicitamos sean tenidos en cuenta dentro de la construcción de tan importante documento, ya que la expedición del mismos tendrá un impacto directo sobre el sector.

Agradeciendo la atención prestada, quedamos atentos a cualquier información adicional que usted o su equipo de trabajo consideren necesarios.

Me despido con sentimientos de consideración y aprecio.

Cordialmente,

A handwritten signature in black ink, appearing to read 'Alberto Samuel Yohai', is written over the printed name and title.

**ALBERTO SAMUEL YOHAI**

Presidente Ejecutivo

Cámara Colombiana de Informática y Telecomunicaciones – CCIT