

Bogotá D.C., Jueves 04 de Agosto de 2017

Doctor

**PABLO FELIPE ROBLEDO**

Superintendente de Industria y Comercio

**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

La Ciudad

**Asunto: Comentarios al proyecto de circular externa por medio de la cual se pretende “Adicionar un Capítulo Tercero al Título V de la Circular Única – Transferencia de datos personales a Terceros Países.”**

---

Apreciado doctor Robledo,

Desde la Cámara Colombiana de Informática y Telecomunicaciones – CCIT, reconocemos el esfuerzo y la labor de la Superintendencia de Industria y Comercio – SIC, que ha realizado en aras de construir de manera conjunta el proyecto de Circular Única, a través de la cual se pretende establecer un adecuado nivel de protección, dentro de la transmisión de datos personales.

En líneas con lo anterior, y atendiendo a la amable invitación que se hace para presentar comentarios al proyecto en mención, desde la industria nos permitimos exponer los siguientes:

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

Desde la industria agradecemos que se haya incluido dentro de la lista de países que cuentan con un nivel adecuado de protección de datos, a los Estados Unidos de América. Sin embargo, dentro del fundamento legal del proyecto de circular se menciona, que en el 2013, la Superintendencia de Industria y Comercio contrató un estudio con una firma de abogados para el análisis sobre la aplicación en Colombia de las normas de transferencia internacional de datos personales, y se desarrolló dentro del mismo una lista no exhaustiva de países, que según el análisis realizado gozaban de un nivel adecuado de protección.

Igualmente, dentro del fundamento legal se establece que:

*“De otra parte, dicho listado contiene también a México, República Corea, Costa Rica, Serbia, Perú, Noruega, Islandia y Estados Unidos, este último en relación con las empresas que se adhirieron al marco “Safe Harbor” o Puerto Seguro, el cual fue reemplazado en el 2016 por el marco “Privacy Shield” o Escudo de Privacidad.”*



En línea con lo anterior, y con el fin de brindarle mayor claridad al texto propuesto, por la Superintendencia de Industria y Comercio, respetuosamente solicitamos que se elimine del fundamento legal la frase referida a *"este último en relación con las empresas que se adhirieron al marco "Safe Harbor" o Puerto Seguro, el cual fue reemplazado en el 2016 por el marco "Privacy Shield" o Escudo de Privacidad."* Lo anterior, evitará la creación de confusiones de interpretación de la misma.

Adicional a ello, consideramos fundamental que se haga referencia dentro del texto de la norma tanto de la transmisión como de la transferencia de datos. Lo anterior, toda vez que la protección que un país otorga para la transferencia se aplica de manera general para la transmisión lo que permitirá eliminar las dudas que actualmente existen en relación con la aplicación de ambas figuras.

Por otro lado, es importante que dentro del texto de la misma se haga referencia sobre la aplicabilidad de la circular dentro de las entidades públicas, ya que actualmente existen varias dudas sobre la aplicabilidad de la misma dentro de estas. En virtud de ello respetuosamente, solicitamos que se haga dicha aclaración.

Finalmente, es fundamental para la industria conocer el mecanismo a través del cual la Superintendencia de Industria y Comercio evalúa si un país cumple o no con los estándares adecuados de protección de datos. Por ello, respetuosamente solicitamos que se haga una aclaración dentro del documento, en donde se especifique cuáles son los criterios adoptados por la entidad para la realización de la inclusión de los países dentro de la lista propuesta.

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

### **Comentarios al numeral 3.2 del numeral 3 del proyecto**

#### **"3. Instructivo**

Adicionar un Capítulo Tercero al Título V de la Circular Única, sobre transferencia internacional de datos personales, el cual quedará así:

#### ***"CAPÍTULO 3: TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES.***

*(...)*

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

*Teniendo en cuenta los estándares señalados en el numeral 3.1 anterior y el análisis efectuado por la Superintendencia, garantizan un nivel adecuado de protección los*



*siguientes países: Alemania; Austria; Bélgica; Bulgaria; Chipre; Costa Rica; Croacia; Dinamarca; Eslovaquia; Eslovenia; Estonia; España; Estados Unidos de América; Finlandia; Francia; Grecia; Hungría; Irlanda; Islandia; Italia; Letonia; Lituania; Luxemburgo; Malta; México; Noruega; Países Bajos; Perú; Polonia; Portugal; Reino Unido; República Checa; República de Corea; Rumania; Serbia; Suecia; y los países que han sido declarados con nivel adecuado de protección por la Comisión Europea.*

*La Superintendencia de Industria y Comercio ejercerá, en cualquier tiempo, su capacidad regulatoria para revisar la lista anterior y proceder a incluir a quienes no hacen parte de la misma o para excluir a quien se considere conveniente, de acuerdo con los lineamientos establecidos en la ley.*

*(...)"*

Si bien reconocemos y celebramos la inclusión, dentro del listado de países que cuentan con un nivel adecuado de protección de datos, de los Estados Unidos de América, vemos con preocupación que países como Brasil, Chile y Ecuador, que cuentan con un marco normativo en materia de protección de datos personales, no se encuentran dentro de dicho listado.

Adicional a ello, recalcamos que las autoridades de protección de datos de Brasil, están ejerciendo una adecuada vigilancia y control en relación con la protección de datos personales. Por dicha labor se destaca la Agencia de Protección al Consumidor de este país, quien en 2014 multó a Oi SA, compañía brasilera de telecomunicaciones, como consecuencia de vender datos de suscriptores a empresas de publicidad en línea que generaba anuncios personalizados.

Igualmente recordamos que Brasil cuenta con el siguiente cuerpo normativo en materia de protección de datos personales:

#### ***"Leyes Generales***

*Brasil ha realizado un esfuerzo mayor para generar regulaciones que aseguren los derechos civiles respecto de internet (que se encuentran incluidos en el Marco Civil de Derechos Civiles para el Internet)*

*La Corte Federal ha definido dos derechos fundamentales que implican un alto grado de protección de la privacidad. Bajo el artículo 5, Secciones X y XII de la Constitución Federal se determina la inviolabilidad de la privacidad y la vida privada, y se garantiza el secreto de la correspondencia y las comunicaciones telegráficas, de datos y telefónicas.*

#### ***Leyes Sectoriales***

*Existen niveles substantivos de protección en varios campos, bajo leyes sectoriales.*



*La principal es, como ya se mencionó el Marco Civil, que incluye una sección que regula los aspectos de datos personales procesados en línea por medio de proveedores de conexión y por proveedores de aplicaciones de internet. El Marco Civil protege los datos personales, los contenidos de las comunicaciones privadas y los registros de acceso relacionados tanto con conexiones a internet y a las aplicaciones. Esta regulación incluye cualquier operación relacionada con la colección, almacenaje, retención, tratamiento y comunicación de los datos personales cuando al menos una de éstas sucede en Brasil.*

*Tanto la Constitución Federal como el Marco Civil aplican tanto a individuos y entidades brasileños y extranjeros viviendo en el territorio brasileño.*

*Adicionalmente, existen regulaciones adicionales de protección de datos en:*

- *Código de Protección del Consumidor. - incluyendo la protección de datos personales incluidos en las bases de datos (más que nada respecto a información crediticia).*
- *Código de Deudores Cumplidos. - relacionado a la recolección, uso y compartición de datos registrados en las bases de datos de personas que pagan cumplidamente.*
- *Código Fiscal. – incluye la secrecía de los impuestos.*
- *Código de Secreto Bancario. – respecto al secreto de operaciones bancarias.*

*Código de Acceso a la Información. – respecto a los datos personales registrados en bases de datos públicas.”<sup>1</sup>*

Finalmente, vale la pena indicar que Ecuador también cuenta con varias normas que cumplen con los mejores estándares en materia de protección de los datos personales, al interior de su ordenamiento jurídico. Tal y como se describe a continuación.

#### **“Constitucion Política.**

##### **Art.66.**

*19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, **archivo**, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.*

*20. El derecho a la intimidad personal y familiar.*

*(...)*

#### **LEY ORGÁNICA DE TELECOMUNICACIONES (“LOT”).**

---

<sup>1</sup> [https://uk.practicallaw.thomsonreuters.com/4-520-1732?originationContext=document&transitionType=DocumentItem&contextData=\(sc.Default\)&firstPage=true&bhcp=1](https://uk.practicallaw.thomsonreuters.com/4-520-1732?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true&bhcp=1)



**(R.O.S. 439 DE 18 FEBRERO 2015)**

**Art. 78.-** *Derecho a la intimidad. Para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal. Para tal efecto, las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos de carácter personal de conformidad con la ley. Dichas medidas incluirán, como mínimo:*

*La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley. 2. La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos. 3. La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales. 4. La garantía de que la información suministrada por los clientes, abonados o usuarios no será utilizada para fines comerciales ni de publicidad, ni para cualquier otro fin, salvo que se cuente con el consentimiento previo y autorización expresa de cada cliente, abonado o usuario. El consentimiento deberá constar registrado de forma clara, de tal manera que se prohíbe la utilización de cualquier estrategia que induzca al error para la emisión de dicho consentimiento.*

**Art. 82.-** *Uso comercial de datos personales. Las y los prestadores de servicios no podrán usar datos personales, información del uso del servicio, información de tráfico o el patrón de consumo de sus abonados, clientes o usuarios para la promoción comercial de servicios o productos, a menos que el abonado o usuario al que se refieran los datos o tal información, haya dado su consentimiento previo y expreso. Los usuarios o abonados dispondrán de la posibilidad clara y fácil de retirar su consentimiento para el uso de sus datos y de la información antes indicada. Tal consentimiento deberá especificar los datos personales o información cuyo uso se autorizan, el tiempo y su objetivo específico. Sin contar con tal consentimiento y con las mismas características, las y los prestadores de servicios de telecomunicaciones no podrán comercializar, ceder o transferir a terceros los datos personales de sus usuarios, clientes o abonados.*

(...)

## **REGLAMENTO GENERAL A LA LEY ORGANICA DE TELECOMUNICACIONES ("RGLOT")**

**(Registro Oficial Suplemento # 676 de 25 de enero de 2016)**

**Art. 120.-** *Garantía de protección de datos personales.- Los prestadores de servicios del régimen general de telecomunicaciones tienen prohibido ejecutar u omitir acciones que violen la garantía de protección de datos personales, esto es, provocar la destrucción, la pérdida, la alteración, la revelación o el acceso no autorizado de datos personales, transmitidos, almacenados o tratados en la prestación de servicios de*



*telecomunicaciones, conforme el alcance, los procedimientos o protocolos previstos en la LOT, su Reglamento General y las regulaciones emitidas por la ARCOTEL para el efecto. La violación de esta garantía dará lugar a la imposición de las sanciones previstas en el ordenamiento jurídico.*

**Art. 121.- Uso comercial.-** Los datos personales que los usuarios proporcionen a los prestadores de servicios del régimen general de telecomunicaciones no podrán ser usados para la promoción comercial de servicios o productos, inclusive de la propia operadora; salvo autorización y consentimiento expreso del usuario.

*Para tal fin, los prestadores de servicios deberán solicitar a sus usuarios su consentimiento expreso, en un instrumento separado y distinto al contrato de prestación de servicios a través de medios físicos o electrónicos, para que la prestadora de servicios del régimen general de telecomunicaciones pueda utilizar comercialmente sus datos personales. En dicho instrumento se deberá dejar constancia expresa de los datos personales o información que están expresamente autorizados; el plazo de la autorización y el objetivo que esta utilización persigue. Sin perjuicio de lo anterior se considerarán públicos los datos contenidos en las guías telefónicas de telefonía fija, no obstante lo cual los abonados tendrán derecho a que se excluyan gratuitamente sus datos personales de dichas guías.*

*La ARCOTEL establecerá los mecanismos y emitirá las regulaciones correspondientes a fin de precautelar el secreto de las comunicaciones y de la información que se trasmite a través de redes de telecomunicaciones, así como la seguridad de los datos personales y de las redes.*

(...)

#### **LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS ("LSNRDP").**

*(Registro Oficial Suplemento # 162 de 31-Marzo-2010)*

**Art. 6.- Accesibilidad y confidencialidad.-** Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.

*El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial. También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado. La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos. Para acceder a la información sobre el patrimonio de las personas el solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará de la misma y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento*



*de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer. La Directora o Director Nacional de Registro de Datos Públicos, definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad.*

## **CODIGO ORGANICO INTEGRAL PENAL, COIP ("COIP").**

**(R.O.S. 180 10 DE FEB 2014, ULTIMA MOD 12 DE SEPTIEMBRE DE 2014)**

**Art. 178.- Violación a la intimidad.-** *La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.*

**Art. 229.- Revelación ilegal de base de datos.-** *La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.*

*Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.*

### **Ley de Comercio Electrónico, Firmas y Mensajes de Datos**

**Art. 9.- Protección de datos.-** *Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.*



*Para el caso de Ecuador, las anteriores normas permiten concluir que este país sí cuenta con los elementos necesarios para garantizar un nivel adecuado de protección de datos personales, ya que su legislación cuenta con derechos y obligaciones de las partes, por ejemplo, del titular del dato y de autoridades que efectivamente protegen el uso de los datos como es el caso de la ARCOTEL.”*

Teniendo en cuenta lo anterior, respetuosamente se solicita la inclusión de Argentina, Brasil, Chile y Ecuador dentro de la lista de países que cuentan con un adecuado nivel de protección de datos personales.

Así pues, ponemos a consideración la siguiente redacción de texto:

### **“3. Instructivo**

Adicionar un Capítulo Tercero al Título V de la Circular Única, sobre transferencia internacional de datos personales, el cual quedará así:

#### **“CAPÍTULO 3: TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES.**

(...)

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

*Teniendo en cuenta los estándares señalados en el numeral 3.1 anterior y el análisis efectuado por la Superintendencia, garantizan un nivel adecuado de protección los siguientes países: Alemania; Austria; Bélgica; **Brasil**; Bulgaria; **Chile**; Chipre; Costa Rica; Croacia; Dinamarca; **Ecuador**; Eslovaquia; Eslovenia; Estonia; España; Estados Unidos de América; Finlandia; Francia; Grecia; Hungría; Irlanda; Islandia; Italia; Letonia; Lituania; Luxemburgo; Malta; México; Noruega; Países Bajos; Perú; Polonia; Portugal; Reino Unido; República Checa; República de Corea; Rumania; Serbia; Suecia; y los países que han sido declarados con nivel adecuado de protección por la Comisión Europea.*

*La Superintendencia de Industria y Comercio ejercerá, en cualquier tiempo, su capacidad regulatoria para revisar la lista anterior y proceder a incluir a quienes no hacen parte de la misma o para excluir a quien se considere conveniente, de acuerdo con los lineamientos establecidos en la ley.*

(...)”

### **Comentarios al párrafo 3 del numeral 3.1 del proyecto de circular**



### **"3. Instructivo**

Adicionar un Capítulo Tercero al Título V de la Circular Única, sobre transferencia internacional de datos personales, el cual quedará así:

#### **"CAPÍTULO 3: TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES.**

(...)

***Parágrafo Tercero:** El simple tránsito transfronterizo o redirección de datos no comporta una transferencia de datos a otros países."*

Si bien se establece dentro del parágrafo que el simple tránsito transfronterizo de datos no implica una transferencia de datos a otros países, consideramos importante que se exprese de manera clara dentro del texto cuáles serían sus efectos. En virtud de lo anterior, ponemos a consideración la siguiente redacción de texto:

### **"3. Instructivo**

Adicionar un Capítulo Tercero al Título V de la Circular Única, sobre transferencia internacional de datos personales, el cual quedará así:

#### **"CAPÍTULO 3: TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES.**

(...)

***Parágrafo Tercero:** El simple tránsito transfronterizo o redirección de datos no comporta una transferencia de datos a otros países, y por tanto no serán aplicables las disposiciones previstas en la presente circular."*

Finalmente, si bien los mecanismos propuestos dentro del proyecto de circular tienen por objeto garantizar los niveles adecuados de protección de datos personales, consideramos que dichos mecanismos por si solos no proveen toda la flexibilidad requerida hoy en día para la transferencia internacional de datos personales. Por ello, es importante tener en cuenta que existen mecanismos adicionales que garantizan igualmente un nivel adecuado de protección, como lo son las "Reglas Corporativas" o BCR por sus siglas en inglés; mecanismos ampliamente aceptados a nivel internacional que garantizan un nivel adecuado de protección de datos que se transfieren, incluso hacia países que disponen de leyes mínimas de protección de datos.



Ejemplo de los mecanismos anteriormente nombrados son; a) Cláusulas de Contratación Estándar; y b) normas corporativas o "Reglas Corporativas Globales" o BCR por sus siglas en inglés, que son aquellas que contienen un código de conducta de protección de datos personales, jurídicamente vinculantes, a través de las cuales las compañías implementan salvaguardas apropiadas para la transmisión de datos personales al interior de un grupo corporativo. Dentro de estas, se incluyen los principios requeridos por la ley de protección de datos aplicable, así como también los derechos reconocidos por la misma, obligando así legalmente a las compañías a cumplir con dichas reglas.

Estas reglas han probado ser altamente efectivas en procesos de revisión, de capacitación, y garantizan un buen manejo dentro de los procesos de reclamaciones. Igualmente, a través del uso de estas reglas se garantiza la eficiencia e innovación para el flujo de datos a nivel interno de las compañías o grupos empresariales.

En virtud de lo anterior, esperamos haber contribuido de manera positiva con nuestros aportes, y quedamos atentos a resolver cualquier inquietud o solicitud de información adicional que usted o su equipo de trabajo considere pertinente.

Agradeciendo la atención prestada, me suscribo de usted con sentimientos de consideración y aprecio.

Cordialmente,

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

**ALBERTO SAMUEL YOHAI**

Presidente Ejecutivo

Cámara Colombiana de Informática y Telecomunicaciones – CCIT