

Bogotá, diciembre 7 de 2017



Doctor
PABLO FELIPE ROBLEDO DEL CASTILLO
Superintendente de Industria y Comercio
Superintendencia de Industria y Comercio (SIC)

Ref. Solicitudes sobre proyecto de circular para modificar el numeral 3.2. del capítulo 3 del título V de la circular única (Transferencia de datos personales a terceros países).

Estimado doctor Robledo:

Cordial y respetuoso saludo.

En virtud del derecho constitucional de petición me permito presentar las siguientes peticiones respecto del texto del proyecto de circular publicado en el siguiente sitio de la página web de la SIC: <http://www.sic.gov.co/proyectos-de-circulares> y cuya imagen de difusión es la siguiente:

Proyectos de circulares

A screenshot of a web search interface for 'Proyectos de circulares'. On the left is a vertical navigation menu with categories: Constitución Nacional, Normas supranacionales, Leyes, Decretos, Resoluciones, Proyectos de resolución, Circula única, and Circulares. The main content area has a search filter with 'TEMA' set to '- Todos -' and 'AÑOS' set to '2017'. A blue 'FILTRAR' button is visible. Below the filter, the search results show the title: '"MODIFICAR EL NUMERAL 3.2 DEL CAPÍTULO TERCERO DEL TÍTULO V DE LA CIRCULAR ÚNICA" - TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES'. Underneath the title, it says 'Detalles y comentarios' and 'Periodo de publicación: 15 días hábiles a partir de hoy 17 de noviembre y hasta el 7 de diciembre de 2017'.

Hemos estructurado nuestro documento de la siguiente manera:



Tabla de contenido

DE LA PRIMERA PARTE DEL PROYECTO DE CIRCULAR.....	3
Petición No. 1: Excluir a los Estados Unidos de América del listado de países con nivel adecuado de protección de datos y crear alternativas jurídicas para que se transfieran datos a ese país pero garantizando la debida protección de los derechos de los colombianos en los EE.UU	4
DEL PARÁGRAFO PRIMERO DEL PROYECTO DE CIRCULAR	14
Petición No. 2 Incluir en la guía de responsabilidad demostrada de la SIC las medidas apropiadas y efectivas que cualquier Responsable debe implementar para garantizar el debido tratamiento de los datos de los colombianos que son exportados a los países que la SIC considera que tienen nivel adecuado de protección de datos.	14
DEL PARÁGRAFO SEGUNDO DEL PROYECTO DE CIRCULAR	17
Petición No. 3: Eliminar el parágrafo segundo del proyecto de circular porque se deja en manos de los Responsables del tratamiento la labor de tomar decisiones que por ley le corresponden a la SIC	17
DEL PARÁGRAFO CUARTO DEL PROYECTO DE CIRCULAR.....	18
PETICIÓN No 4 : Eliminar el parágrafo cuarto del proyecto de circular porque es ilegal ya que la SIC no puede mediante circular modificar el decreto 1377 de 2013.....	19
Petición No 5: Que la SIC antes de expedir la circular definitiva objeto de estos comentarios solicite concepto sobre su contenido a la Procuraduría General de la Nación y a la Defensoría del Pueblo para que se tenga presente la perspectiva de entidades encargadas de la protección de derecho humanos.	19



DE LA PRIMERA PARTE DEL PROYECTO DE CIRCULAR

CIRCULAR EXTERNA No.

Bogotá D.C.

Para: RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES

Asunto: Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única

1. Objeto

Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única con el fin de incluir un país dentro de la lista de países contenida en dicho numeral, los cuales cuentan con un nivel adecuado de protección de datos personales de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio.

3. Instructivo

Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única, sobre transferencia de datos personales, el cual quedará así:

“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 esta 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; Japón; 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 el 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.



Petición No. 1: Excluir a los Estados Unidos de América del listado de países con nivel adecuado de protección de datos y crear alternativas jurídicas para que se transfieran datos a ese país pero garantizando la debida protección de los derechos de los colombianos en los EE.UU

JUSTIFICACIÓN: Es importante recordar que los artículos 1, 2 y 123 de la Constitución son claros en ordenar que: I) en Colombia debe prevalecer el interés general ; II) son fines esenciales del Estado garantizar la efectividad de los derechos y facilitar la participación de todos en la decisiones que nos afectan; III) Las autoridades de la República están instituidas para proteger, entre otros, los derechos y las libertades, y IV) los servidores públicos están al servicio de la comunidad y deben ejercer sus funciones en la forma prevista por la Constitución, la ley y el reglamento.

Estados Unidos de América no cumple los requisitos jurídicos que exige la ley 1581 de 2012 para ser considerado como país con nivel adecuado de protección de datos tal y como lo ilustramos en la siguiente tabla:

El artículo 26 de la ley 1581 de 2012 prohíbe la transferencia de datos personales *“a países que no proporcionen niveles adecuados de protección de datos”* y EXIGE que los estándares que debe cumplir el país extranjero **“en ningún caso podrán ser inferiores”** a los que exige la ley 1581 de 2012.

PROTECCIÓN DE DATOS PERSONALES			
Concibe la protección de datos como un derecho fundamental de naturaleza constitucional?	Si	No	
Exige la autorización previa, expresa e informada de las personas para recolectar y tratar sus datos personales?	Si	No	
Cuenta con una norma general sobre tratamiento de datos?	Si	No	
Comprende normas sectoriales?	Si	Si	
Considera necesaria la existencia de autoridad autónoma, independiente y especializada en la protección de datos personales?	Si	No	
Acción de tutela para proteger los derechos del titular del dato?	Si	No	
Mecanismo de consultas y reclamos en los mismos términos de los artículos 14-15 de la L1581 de 2012	Si	No	

Tabla 1: Comparación de aspectos jurídicos de la regulación colombiana y los Estados Unidos de América respecto de la protección de datos personales.



En síntesis, la regulación de los EE.UU ofrece un nivel inferior de protección a los titulares de los datos respecto del que exige la Constitución de la República de Colombia y la ley 1581 de 2012.

Es de público conocimiento que el actual gobierno de los EE.UU ha tomado medidas que disminuyen la protección de los datos de los extranjeros. Por eso, no entendemos como la SIC como autoridad de protección de datos decide que ese país tiene nivel adecuado de protección de datos sabiendo que las medidas del citado gobierno afectan negativamente a los colombianos y las colombianas cuando su información ingrese a territorio de los EE.UU.

Estas imágenes de noticias son muy dicentes por si solas y no merecen mayor explicación :



Trump elimina la protección de datos de extranjeros en EE.UU.

El decreto podría dejar en el aire el pacto con Europa conocido como Escudo de la Privacidad.

<http://www.eltiempo.com/mundo/euu-y-canada/trump-elimina-la-proteccion-de-datos-de-extranjeros-en-ee-uu-72126>

Donald Trump ordena eliminar la protección de datos para ciudadanos no estadounidense

Por: **R3D: Red en Defensa de los Derechos Digitales** - 26 enero, 2017

El presidente de los Estados Unidos, Donald Trump, firmó ayer un decreto para eliminar las protecciones contempladas en la Ley de Privacidad de los EE.UU para cualquier persona que no sea ciudadana de este país.

La orden ejecutiva "Incrementando la Seguridad Pública al Interior de los Estados Unidos" borra de golpe las protecciones a los datos de millones de ciudadanos extranjeros que circulan diariamente por redes y servidores estadounidenses, además de aquellos que viven en el país norteamericano, pero no que no tienen ese estatus.

"Las agencias deben, hasta una extensión consistente con la ley aplicable, asegurar que sus políticas de privacidad excluyan a personas que no son ciudadanos estadounidenses o residentes permanentes legales de las protecciones de la Ley de Privacidad respecto a la información personal identificable", se puede leer en la Sección 14 de la orden.

Tomado de: <https://r3d.mx/2017/01/26/donald-trump-ordena-eliminar-la-proteccion-de-datos-para-ciudadanos-no-estadounidense/>

Adicionalmente importantes organizaciones de protección de derechos humanos han puesto de presente los efectos negativos de las decisiones del gobierno norteamericano. Nos parece que esto es algo que no debe pasar por alto la SIC como autoridad de protección de los datos de los colombianos. Esta es la parte pertinente de la comunicación:



WASHINGTON
LEGISLATIVE OFFICE



February 28, 2017

Donald F. McGahn
Assistant to the President and White House Counsel
1600 Pennsylvania Ave. NW, 2nd Floor, West Wing
Washington, D.C. 20500

Re: Privacy Implications of Executive Order 13768: Enhancing Public Safety in the Interior of the United States

Dear Mr. McGahn,

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

FAIZ SHAKIR
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

In recent weeks, President Trump has issued several executive orders that represent an attack on the rights of immigrants and foreigners—including the right to privacy that has been protected for decades in prior Republican and Democratic administrations. Specifically, Section 14 of President Trump’s Executive Order 13768, signed January 25, 2017, and entitled “Enhancing Public Safety in the Interior of the United States (“Section 14” or the “EO”) states that: “[a]gencies 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” (emphasis added).¹ This dramatic shift in policy will create an implementation nightmare that threatens the privacy rights of immigrants, foreign residents, and U.S. citizens; raises multiple constitutional and legal concerns; and calls into question whether the U.S. is meeting its obligations under existing international agreements. Thus, we urge you to swiftly reverse this policy change and recognize that it cannot be achieved “consistent with applicable law.”

Se suma a lo anterior lo señalado en publicaciones importantes del mundo como lo es la Universidad de Harvard cuya nota transcribimos para que sea considerado por la SIC:



On internet privacy, be very afraid

HARVARDgazette

August 24, 2017 | ✓ ||

'Surveillance is the business model of the internet,' Berkman and Belfer fellow says (...)

By Liz Mineo, Harvard Staff Writer

In fact, internet users in the United States have fewer privacy protections than those in other countries. In April, Congress voted to allow internet service providers to collect and sell their customers' browsing data. By contrast, the European Union hit Google this summer with a \$2.7 billion antitrust fine.

<https://news.harvard.edu/gazette/story/2017/08/when-it-comes-to-internet-privacy-be-very-afraid-analyst-suggests/>

Nótese que la Corte Constitucional ha dicho que cuando se transfieren datos a otros países se deben evitar lesionar los derechos de las personas. Incluir a EE.UU en ese listado hace todo lo contrario debido a que se crean riesgos a los ciudadanos dadas las particularidades y observaciones precedentes.

Esto dijo la Corte sobre el tema en la sentencia C-748 de 2011:



C-748 de 2011

- “Debido a la necesidad de circular internacionalmente datos personales **se han dispuesto reglas que deben observarse con miras a que los esfuerzos internos de protección de cada país no sean inútiles al momento de su exportación a otros países.**” (numeral 2.25.3.1)
- “objetivo de no impedir el tratamiento de los datos **pero evitando lesionar derechos de las personas con ocasión del mismo**, derechos constitucionales como el derecho a la intimidad. (numeral 2.25.3.1)



De otra parte, consideramos que la medida por la SIC no aprueba un juicio de proporcionalidad en los términos que ha establecido la Corte Constitucional en la sentencia C-309 de 1997 tal y como se pone de presente en la siguiente ilustración:

El proyecto de circular reprueba juicio de proporcionalidad de la Corte Constitucional



C-309 de 1997

El proyecto de circular persigue una finalidad constitucional?



El proyecto de circular es adecuada –sirve- para lograr el fin propuesto?



El proyecto de circular es necesaria: No existen medidas alternativas menos lesivas a los derechos de las personas?



El proyecto de circular es proporcional dado que no sacrifica valores y principios de mayor peso como la protección efectiva del debido tratamiento de datos personales de 49,412,025 colombianos (as)? -riesgos a los derechos de personas vs eventuales beneficios / riesgos muy fuertes frente a beneficios menores-



No debe perderse de vista que la SIC tuvo en cuenta un estudio que concluyó que los EE.UU tienen nivel adecuado de protección. No obstante, ese documento es francamente muy endeble y contradictorio. Veamos muy brevemente por que afirmamos lo anterior:

El estudio es endeble porque la única “regulación” que cita de ese país es el acuerdo de puerto seguro (Safe Harbor) de EE.UU y la Unión Europea¹ como se puede ver a continuación:

¹ Cfr. Págs. 66 y 67 del estudio publicado por la SIC en su página web



País (Normas)	Obligaciones de las partes	Derechos del titular	Principios sobre los datos (Calidad del dato y seguridad técnica)	Procedimiento de protección de datos (Mecanismos y Autoridades)
Estados Unidos de Puerto Seguro (“Acuerdo de Puerto Seguro”)	Se establecen unos deberes para las organizaciones que reciban datos personales de países pertenecientes a la Unión Europea, todos ellos encaminados a que se garanticen los principios contenidos en el acuerdo.	Se establece el derecho de acceso a la información.	Se establece el principio de seguridad de acuerdo con el cual, las organizaciones que administren información personal, deberán tomar las debidas precauciones para protegerla de pérdida, alteración, destrucción, acceso indebido, etc. Se establece un principio de integridad de los datos de acuerdo con el cual, la información personal recolectada debe ser relevante para los propósitos para los cuales se va a usar.	Se establece el rol de las autoridades de protección de datos, y cómo las organizaciones que administren datos, deben cooperar con ellas.

No obstante, el estudio no tuvo en cuenta que ese acuerdo no es una norma de los EE.UU y que fue declarado inválido por el Tribunal de Justicia mediante sentencia del 6 de octubre de 2015 (Asunto C-364/14) cuya parte resolutive dice lo siguiente:



InfoCuria - Jurisprudencia del Tribunal de Justicia

En virtud de todo lo expuesto, el Tribunal de Justicia (Gran Sala) declara:

- 1) El artículo 25, apartado 6, de la de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en su versión modificada por el Reglamento (CE) nº 882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003, entendido a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, en su versión modificada, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.
- 2) La Decisión 2000/520 es inválida.

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=81464>



La Decisión 2000/520 fue reemplazada por el Privacy Shield Framework pero sigue siendo un instrumento únicamente aplicable a algunas empresas de los EE.UU. —no todo el territorio de ese país— y no vincula ni crea obligaciones de dichas empresas frente a empresas o entidades públicas colombianas. En suma, el “Escudo de Privacidad” no beneficia a los titulares de los datos cuya información es enviada desde Colombia a los EE.UU.

El estudio también es contradictorio porque en la página 20 dice que ese acuerdo solo avala a las empresas que se comprometen a cumplirlo ante la Federal Trade Commission, es decir que el autor del estudio reconoce que el nivel adecuado no es para todo los EE.UU. como país sino para algunas empresas de ese Estado, lo cual es muy diferente. No obstante, el autor del estudio concluye que EE.UU. tiene nivel adecuado de protección de datos. Veamos lo que dice el estudio:

ESTUDIO SOBRE LA APLICACIÓN EN COLOMBIA DE LAS NORMAS SOBRE TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Las organizaciones que decidan participar en el programa Safe Harbor deben cumplir y declarar públicamente que lo hacen. Para garantizar los beneficios del programa puerto seguro, las organizaciones deben ratificar su autocertificación cada año ante el Departamento de Comercio de Estados Unidos, lo que demuestra que siguen cumpliendo con los requisitos del programa Safe Harbor. También se requiere que la organización en su declaración de política de privacidad publicada, señale expresamente que se adhiere a los principios de puerto seguro.¹³

Cualquier empresa estadounidense que quiera ser receptora de transferencias internacionales de datos de carácter personal procedentes de la Unión Europea, tiene que adherirse al programa Safe Harbor. Si una organización está adherida a dicho acuerdo, se considera que cumple con los principios de privacidad necesarios, y el destino es “confiable”.

Pág. 20

En suma, el estudio que usa la SIC está desactualizado, es incompleto y contradictorio. Pese a lo anterior, llama mucho la atención que la SIC, a pesar de ser una autoridad experta en protección de datos no hiciera ningún reparo al estudio y lo aplicara automáticamente a pesar de las notorias falencias y debilidades que hemos mencionado. En efecto, esto es lo que ha dicho la SIC sobre el cuestionado estudio:



En el 2013, la Superintendencia de Industria y Comercio contrató un estudio con una firma de abogados sobre la aplicación en Colombia de las normas sobre transferencia internacional de datos personales. Con fundamento en lo establecido en el artículo 26 de la Ley 1581 de 2012 y la sentencia de la Corte Constitucional antes citada, dentro del estudio ya referido se elaboró una lista no exhaustiva de países que, según el análisis efectuado por dicha firma tienen un nivel adecuado de protección. Para el efecto, en dicho estudio se tuvieron en cuenta las normas de dichos países y lo regulado por estas frente a los principios que rigen el tratamiento de datos personales, los derechos de los titulares, los deberes de Responsables y Encargados de Tratamiento, los mecanismos dispuestos para hacer efectivos esos derechos y la existencia de autoridades que garanticen de manera efectiva los mismos y hagan cumplir la ley.

(....)

De otra parte, dicho listado contiene también a México, República de Corea, Costa Rica, Serbia, Perú, Noruega, Islandia y Estados Unidos.

Página 3

Lo anterior es lamentable porque la decisión de la SIC se fundamenta en un estudio muy controvertible por su contenido y ello afecta a los ciudadanos colombianos porque ese documento fue decisivo para concluir que EE.UU tienen nivel adecuado de protección.

De otra parte, la SIC es la única autoridad de protección de datos del mundo que declaró a los EE.UU como país con nivel adecuado de protección de datos. Si bien la SIC puede concluir lo que considere conveniente, ello no debe hacerse de cualquier manera por dos razones: En primer lugar, lo que está de por medio es la protección de un derecho fundamental de más de 49 millones de colombianos (as). En segundo lugar, la SIC es la autoridad de protección de datos personales y como tal su mandato legal es proteger a los ciudadanos. Por eso, la SIC debe abstenerse de tomar decisiones que pongan en riesgo los derechos de las personas como lo es, precisamente, incluir a EE.UU dentro del listado de países con nivel adecuado de protección.

La SIC no ha presentado argumentos jurídicos suficientes ni convincentes para haber tomado una decisión tan importante. De hecho, autoridades de protección de datos de otros países no han incluido a los EE.UU dentro del listado de Estados con nivel adecuado y ello no ha afectado los negocios, ni constituye una barrera a la economía digital. Este es el caso, por ejemplo, de Argentina y Uruguay cuyas decisiones transcribimos:



Argentina no incluyó a EE.UU en el listado de países con nivel adecuado



MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES
Disposición 60 - E/2016 Ciudad de Buenos Aires, 16/11/2016

- ARTÍCULO 3° — A los fines de la aplicación de la presente disposición se consideran países con legislación adecuada a los siguientes: Estados miembros de la UNIÓN EUROPEA y miembros del espacio económico europeo (EEE), CONFEDERACIÓN SUIZA, GUERNSEY, JERSEY, ISLA DE MAN, ISLAS FEROE, CANADÁ sólo respecto de su sector privado, PRINCIPADO DE ANDORRA, NUEVA ZÉLANDA, REPÚBLICA ORIENTAL DEL URUGUAY y ESTADO DE ISRAEL sólo respecto de los datos que reciban un tratamiento automatizado. Esta enumeración será revisada periódicamente por esta Dirección Nacional, publicando la nómina y sus actualizaciones en su sitio oficial en Internet.
- <http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm>

Uruguay no incluye a EE.UU dentro del listado de países con nivel adecuado de protección



CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

RESOLUCION No.	Expediente No.
17 009 05 009	

Montevideo, 12 de junio de 2009

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

- 1) Establecer que se consideran países apropiados para las transferencias internacionales de datos, aquellos que a juicio de esta Unidad, cuentan con normas de protección adecuadas y medios para asegurar su aplicación eficaz.
- 2) Declarar que en virtud de lo establecido en el numeral precedente, se encuentran comprendidos los países miembros de la Unión Europea y aquellos que la Comisión Europea considere garantizan las condiciones antes indicadas, en base a la normativa citada en la presente resolución.

De otra parte, la decisión de incluir a los EE.UU como país con nivel adecuado de protección de datos también pone en riesgo los intereses del Estado Colombiano porque la expedición de la ley 1581 de 2012, como puede leerse en la exposición de motivos que dio origen a la



misma, buscaba, entre otras, que Europa considerara a Colombia como país con nivel adecuado de protección de datos.

Este objetivo del Estado colombiano puede desdibujarse porque Europa ahora tendrá en cuenta lo atinente a las transferencias internacionales ulteriores. En otras palabras, Colombia podría convertirse en una especie de “paraíso informático” al cual remiten datos de todas partes del mundo para que desde Colombia se reenvíe esos datos a EE.UU.

Lo anterior lo resumimos en la siguiente gráfica:

Efecto internacional de la decisión de la SIC frente a Europa



- La circular 5 de 2017 de la SIC pone en riesgo que Europa declare a Colombia como país que NO tiene nivel adecuado de protección de datos, porque la Comisión Europea considerará lo atinente a las transferencias ulteriores:

Artículo 45. Transferencias basadas en una decisión de adecuación: (...)

- 2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:
- a) *el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos”*



DEL PARÁGRAFO PRIMERO DEL PROYECTO DE CIRCULAR



CIRCULAR EXTERNA No.

Bogotá D.C.

Para: RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES**Asunto: Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única****1. Objeto**

Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única con el fin de incluir un país dentro de la lista de países contenida en dicho numeral, los cuales cuentan con un nivel adecuado de protección de datos personales de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio.

3. Instructivo

Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única, sobre transferencia de datos personales, el cual quedará así:

Parágrafo Primero: Sin perjuicio de que las transferencias de datos personales se realicen a países que tienen un nivel adecuado de protección, los Responsables del Tratamiento, en virtud del principio de responsabilidad demostrada, deben ser capaces de demostrar que han implementado medidas apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia.

Petición No. 2 Incluir en la guía de responsabilidad demostrada de la SIC las medidas apropiadas y efectivas que cualquier Responsable debe implementar para garantizar el debido tratamiento de los datos de los colombianos que son exportados a los países que la SIC considera que tienen nivel adecuado de protección de datos.

La decisión de la Superintendencia de Industria y Comercio (SIC) representa una de las principales políticas públicas en materia de protección de los derechos humanos de las personas. Como tal, debe analizarse detalladamente porque no sólo adoptó decisiones



generadoras de graves riesgos a más de 49 millones de colombianos (as) sino que emitió órdenes cuyo cumplimiento real y efectivo será muy difícil sin las instrucciones concretas de esa entidad.

Como es sabido, la Corte Constitucional ha manifestado que *“debido a la necesidad de circular internacionalmente datos personales se han dispuesto reglas que deben observarse con miras a que los esfuerzos internos de protección de cada país no sean inútiles al momento de su exportación a otros países.”* y es necesario adoptar medidas con el *“objetivo de no impedir el tratamiento de los datos pero evitando lesionar derechos de las personas con ocasión del mismo, derechos constitucionales como el derecho a la intimidad”*. (Sentencia C248 de 2011. numeral 2.25.3.1). En otras palabras, de poco o nada sirve que en Colombia tengamos un sistema de protección de datos si enviamos esa información a países con un nivel de protección inferior al que ofrecen las regulaciones y las instituciones colombianas.

La SIC considera que 48 países del mundo *-incluidos los Estados Unidos-* tiene nivel adecuado de protección de datos. Por eso, se pueden transferir datos de 49 millones de personas a esos Estados y sin autorizaciones de los colombianos.

Para la SIC, la responsabilidad demostrada es una especie de “fórmula mágica” o medida que garantiza que los derechos de los colombianos no sean vulnerados con ocasión o como efecto de las transferencias internacionales. Nos parece acertado pero insuficiente que sólo se recurra a la implementación de ese principio. Creemos que también debió acudir a otras herramientas previstas para dicho efecto como, entre otras, las cláusulas contractuales, las normas corporativas vinculantes o las certificaciones de buenas prácticas.

La [Guía de la SIC del 28 de mayo de 2015 sobre responsabilidad demostrada – accountability-](#) no dice nada sobre las transferencias internacionales *-sólo menciona las transmisiones que son sustancialmente diferentes-*. Dado lo anterior, consideramos necesario que la SIC modifique dicha guía e incluya las instrucciones precisas, útiles y verificables que cualquier Responsable del Tratamiento debe adoptar antes de transferir los datos de los (as) colombianos (as) a otro país.

Esto es necesario por las siguientes razones:

A. La SIC debe dar ejemplo y señalar el camino a seguir en materia de transferencias internacionales y protección efectiva de los derechos de los titulares de los datos . Si dicha entidad exige responsabilidad demostrada a los Responsables del Tratamiento, pues la SIC, como autoridad de protección de datos, debe dar a conocer las *“medidas apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que transfieren a*



otros país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia”.

No nos parece sensato dejar este tema exclusivamente en manos de la Responsables del Tratamiento porque estamos hablando de la protección de derechos constitucionales fundamentales de mas de 49,5 millones de personas.

B. La transferencia internacional de datos vía responsabilidad demostrada es una cuestión novedosa sobre la cual existe mucho desconocimiento. Por eso, a la SIC, como autoridad de protección de datos, le corresponde suplir esas falencias para que no se ponga en riesgo la protección de los derechos de las personas cuyos datos son exportados a otros países.

Sin esas instrucciones de la SIC, cada Responsable del Tratamiento implementaría lo que considere conveniente pero ello no es suficiente porque **lo que está en juego es la real y efectiva protección de los derechos de los colombianos.** La SIC no puede dejar al arbitrio de cada Responsable del Tratamiento la protección de los derechos de las personas cuyos datos son exportados a los 48 países.

C. El principio de responsabilidad demostrada es una medida importada de otros sistemas jurídicos y poco conocida en el país a pesar de la existencia de la guía de la SIC. En la práctica, muchos Responsables del Tratamiento no saben que hacer concretamente. Algunos tienen recursos para acudir a los servicios de empresas especializadas en accountability, pero la mayoría carece de dinero para ese propósito. Así las cosas, la implementación real de la accountability dependerá, en muchos casos, de los recursos económicos de cada empresa, lo cual afectará la protección efectiva de los derechos de las personas cuyos datos son exportados por Responsables del Tratamiento que no tienen dinero.

D. Las instrucciones de la SIC sobre accountability y transferencias internacionales reducirían costos a las empresas *-porque por lo menos saben lo que deben hacer-* y establecerían unos mínimos para tratar de garantizar un cierto nivel de los derechos de las personas cuyos datos serán trasferidos a los 48 países que avaló la SIC.

E. La SIC tiene el deber legal de impartir instrucciones “sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los responsables” a las exigencias de la regulación colombiana (Literal e del artículo 21 de la ley 1581 de 2012). Por eso, **la SIC debería cumplir su función en esta materia y no trasladar su responsabilidad a cada Responsable del Tratamiento que va a exportar datos.**



La SIC no debe perder de vista que de sus decisiones e instrucciones depende la debida protección de los derechos humanos de mas de 49,5 millones de personas.

DEL PARÁGRAFO SEGUNDO DEL PROYECTO DE CIRCULAR



CIRCULAR EXTERNA No.

Bogotá D.C.

Para: RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES

Asunto: Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única

1. Objeto

Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única con el fin de incluir un país dentro de la lista de países contenida en dicho numeral, los cuales cuentan con un nivel adecuado de protección de datos personales de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio.

3. Instructivo

Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única, sobre transferencia de datos personales, el cual quedará así:

Parágrafo Segundo: *Cuando la Transferencia de datos personales se vaya a realizar a un país que no se encuentre dentro de los relacionados en el presente numeral, corresponderá al Responsable del tratamiento que efectuará la transferencia verificar si la operación está comprendida dentro de una de las causales de excepción establecidas en el artículo 26 de la Ley 1581 de 2012, o, si ese país cumple con los estándares fijados en el numeral 3.1 anterior, casos en los cuales podrá realizar la transferencia, o, de no cumplirse ninguna de las*

condiciones anteriores, solicitar la respectiva declaración de conformidad ante esta Superintendencia.

Petición No. 3: Eliminar el parágrafo segundo del proyecto de circular porque se deja en manos de los Responsables del tratamiento la labor de tomar decisiones que por ley le corresponden a la SIC.

Como está redactado el parágrafo, la SIC impone a los Responsables del tratamiento de datos responsabilidades no previstas en la ley 1581 de 2012 que van en detrimento de la protección de los derechos de los ciudadanos porque se deja en manos del exportador de



datos (El Responsable del tratamiento) verificar que el país de destino cumple los estándares fijados por la SIC.

Nótese que se crea un conflicto de intereses porque al exportador de datos lo que le interesa es exportar los datos, pero al mismo se le impone el deber de verificar que ese país cumple unos requisitos para poder exportar datos hacia el mismo. Sobre este tema, solicito que la SIC se remita a las consideraciones que sobre este punto realizó la Corte Constitucional en la sentencia C-1011 de 2008.

En suma preocupa que sea el exportador de la información quien defina si el país de destino cumple unos requisitos para proteger los derechos humanos de los titulares de los datos cuya información será exportada a ese país.

DEL PARÁGRAFO CUARTO DEL PROYECTO DE CIRCULAR

CIRCULAR EXTERNA No.

Bogotá D.C.

Para: RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES

Asunto: Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única

1. Objeto

Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única con el fin de incluir un país dentro de la lista de países contenida en dicho numeral, los cuales cuentan con un nivel adecuado de protección de datos personales de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio.

3. Instructivo

Modificar el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única, sobre transferencia de datos personales, el cual quedará así:

Parágrafo Cuarto: *Es posible realizar la transmisión de datos personales a los países que cuentan con un nivel adecuado de protección de datos personales, en los términos que rigen la transferencia de datos personales”.*



PETICIÓN No 4 : Eliminar el párrafo cuarto del proyecto de circular porque es ilegal ya que la SIC no puede mediante circular modificar el decreto 1377 de 2013.

Con ese párrafo la SIC, como ya lo confirmó por escrito al Congreso de la República, eliminó la necesidad de suscribir el contrato de transmisión internacional de datos cuando el destinatario de la información este ubicado en un país que la SIC considere que tiene nivel adecuado de protección de datos.

Ese párrafo es notoriamente ilegal porque el decreto 1377 de 2013 exige la necesidad de suscribir el contrato de transmisión de datos sin distinguir si la misma se realiza a países con o sin nivel adecuado de protección.

Con el párrafo cuarto la SIC modifica el decreto 1377 de 2013 desconociendo el Estado de Derecho y la jerarquía normativa que existe en Colombia.

Adicionalmente, encontramos que esa decisión también es contradictoria con la doctrina de la SIC porque de una parte exige que se adopten medidas verificables de responsabilidad demostrada y, por otra parte, suprime la necesidad de suscribir contratos, los cuales son, entre otras, un medio probatorio de esas medidas.

No sobre recordar que el artículo 123 de la Constitución ordena que los servidores públicos *“están al servicio del Estado y de la comunidad”* y que deben ejercer *“sus funciones en la forma prevista por la Constitución, la ley y el reglamento.”*. De no eliminarse el párrafo 4 la SIC no estaría obrando dentro de lo que ordena el decreto 1377 de 2013, reglamentario de la ley estatutaria 1581 de 2012.

Petición No 5: Que la SIC antes de expedir la circular definitiva objeto de estos comentarios solicite concepto sobre su contenido a la Procuraduría General de la Nación y a la Defensoría del Pueblo para que se tenga presente la perspectiva de entidades encargadas de la protección de derecho humanos. .

Recalamos la importancia de esta solicitud porque en la decisión de la SIC no sólo debe tenerse en cuenta la Industria y el Comercio sino la protección de los derechos humanos de los colombianos, razón por la cual se hace necesario conocer el concepto de entidades especializadas en ese tema como, por ejemplo, la Procuraduría General de la Nación y la Defensoría del Pueblo.



Le anticipamos nuestra gratitud por su lectura y consideración de estas peticiones y observaciones. Esperamos que la SIC tome decisiones en pro de la protección del derecho fundamental al debido tratamiento de los datos personales de mas de 49 millones de colombianos (as).

Por favor enviar su respuesta a la siguiente dirección de correo electrónico:
nremolin@uniandes.edu.co .

Atentamente,



Nelson Remolina Angarita

CC 13925487

Profesor Asociado y Director del GECTI –*Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática-*

Director del Observatorio CIRO ANGARITA BARÓN sobre la protección de datos en Colombia

Facultad de Derecho

Universidad de los Andes

CC:

Dr. Fernando Carrillo Flórez, Procurador General de la Nación

Dr. Defensor del Pueblo