REPÚBLICA DE COLOMBIA

GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

ISSN 0123 - 9066

AÑO XXVI - Nº 873 Bogotá, D. C., viernes, 29 de septiembre de 2017 EDICIÓN DE 76 PÁGINAS

DIRECTORES: GREGORIO ELJACH PACHECO
SECRETARIO GENERAL DEL SENADO
www.secretariasenado.gov.co

JORGE HUMBERTO MANTILLA SERRANO
SECRETARIO GENERAL DE LA CÁMARA
www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PÚBLICO

SENADO DE LA REPÚBLICA

ACTAS DE COMISIÓN

COMISIÓN PRIMERA CONSTITUCIONAL PERMANENTE

HONORABLE SENADO DE LA REPÚBLICA

ACTA NÚMERO 13 DE 2017

(septiembre 19)

Cuatrienio 2014-2018 - Legislatura 2017-2018

Primer Periodo - Sesión Ordinaria

En la ciudad de Bogotá, D. C., el día diecinueve (19) de septiembre del dos mil diecisiete (2017), se reunieron en el Salón Guillermo Valencia del Capitolio Nacional, previa citación, los miembros de la Comisión Primera del Honorable Senado, con el fin de sesionar.

I

Llamado a lista y verificación del quórum

La Presidencia ejercida por el titular honorable Senador Roosvelt Rodríguez Rengifo, indica a la Secretaría llamar a lista y contestaron los honorables Senadores:

Amín Hernández Jaime

Enríquez Maya Eduardo

Enríquez Rosero Manuel

Gaviria Vélez José Obdulio

Gerléin Echeverría Roberto

López Hernández Claudia

Rodríguez Rengifo Roosvelt

Serpa Uribe Horacio.

En el transcurso de la sesión se hicieron presentes los honorables Senadores:

Andrade Serrano Hernán

Barreras Montealegre Roy Leonardo

Benedetti Villaneda Armando

Galán Pachón Juan Manuel

López Maya Alexánder

Morales Hoyos Viviane

Motoa Solarte Carlos Fernando

Rangel Suárez Alfredo

Valencia Laserna Paloma

Varón Cotrino Germán

Vega Quiroz Doris Clemencia.

La Secretaría informa que se ha registrado quórum deliberatorio.

Siendo las 10:27 a. m., la Presidencia manifiesta:

"Ábrase la sesión y proceda el Secretario a dar lectura al Orden del Día para la presente reunión".

Por Secretaría se da lectura al Orden del Día:

ORDEN DEL DÍA

Cuatrienio 2014 - 2018 Legislatura 2017-2018

Día: martes 19 de septiembre de 2017

Lugar: Salón Guillermo Valencia – Capitolio Nacional Primer Piso

Hora: 10:00 a. m.

I

Llamado a lista y verificación del quórum

II

Consideración y aprobación de actas

Acta número 06 del 15 de agosto de 2017, *Gaceta del Congreso* número 756 de 2017; Acta número 07 del 16 de agosto de 2017, *Gaceta del Congreso* número 757 de 2017; Acta número 08

del 22 de agosto de 2017, *Gaceta del Congreso* número 776 de 2017; Acta número 09 del 23 de agosto de 2017, *Gaceta del Congreso* número 768 de 2017; Acta número 10 del 29 de agosto de 2017; Acta número 11 del 30 de agosto de 2017; Acta número 12 del 12 de septiembre de 2017

III

Citación a los señores Ministros del Despacho y altos funcionarios del Estado

Proposición número 08

En atención a lo previsto en la Circular Externa 005 del 10 de agosto de 2017 y propendiendo por la garantía del derecho fundamental al hábeas data y a la protección de los datos personales de los colombianos en materia de recolección, almacenamiento, uso, circulación y en general cualquier tipo de operaciones efectuadas por empresas norteamericanas, se hace necesario, urgente e impostergable, que de manera inmediata se cite a debate de control político al Ministro de Tecnologías de la Información y las Comunicaciones, doctor David Luna; a la Ministra de Comercio Industria y Turismo, doctora María Lorena Gutiérrez Botero, al Superintendente de Industria y Comercio, doctor Pablo Felipe Robledo y a la Superintendente Delegada para la Protección de Datos, doctora María Claudia Cabiedes Mejía para que respondan por el cuestionario que se anexa.

También invítese al Director del Observatorio Ciro Angarita Barón de Protección de Datos y del GECTI -Grupo de Estudios en Internet, Comercio electrónico, Telecomunicaciones e Informática- de la Universidad de los Andes, doctor Nelson Remolina Angarita; al Director de ACUI, doctor Antonio Medina Gómez; a los representantes de Google Colombia, Microsoft Colombia y Twitter Colombia.

Adicionalmente, le solicito respetuosamente que para este debate se tenga transmisión en vivo del canal institucional del Congreso de la República y demás medios de comunicación con que la corporación cuente.

De los honorables Senadores,

CUESTIONARIO:

1. ¿Existe tratado o convenio vigente y jurídicamente vinculante entre Estados Unidos y Colombia para el tratamiento de datos personales?
2. ¿Existe tratado o convenio vigente y jurídicamente vinculante entre algún otro país y Colombia para el tratamiento de datos personales? En caso afirmativo ¿cuáles son los derechos en cabeza de los titulares de la información, así como los procedimientos y sanciones previstos para proteger el derecho fundamental al hábeas data y a la protección de datos personales?
3. ¿Actualmente algún país extranjero cuenta con autorización para el tratamiento de datos de colombianos? En caso afirmativo informar la reglamentación que rige la transferencia internacional de datos para cada caso.
4. En materia de reciprocidad, ¿Existe algún documento de las autoridades de los Estados Unidos que declaren formalmente a Colombia como un país que tenga nivel adecuado de protección de datos? ¿Existe algún documento de las autoridades de los Estados Unidos que permita que personas naturales o jurídicas ubicadas en territorio colombiano puedan receptar y tratar datos de ciudadanos americanos? De ser así ¿cuáles son las condiciones que deben reunir las personas naturales o jurídicas ubicadas en territorio colombiano para efectuar tratamiento de datos de norteamericanos? Sírvase efectuar análisis comparado entre la regulación a la cual deben someterse los Responsables del Tratamiento de Datos colombianos y las condiciones a las que estarían sujetas las personas naturales o jurídicas americanas Responsables del Tratamiento de Datos.
5. ¿Cómo se ha manejado hasta ahora la recolección, almacenamiento, uso, circulación y en general cualquier tipo de operaciones efectuadas por empresas norteamericanas y que involucran datos de connacionales?
6. Sírvase informar cuáles personas naturales o jurídicas de los Estados Unidos actualmente tratan datos de colombianos, indicando el volumen de información que recolectan, almacenan, usan o circulan.
7. Sírvase remitir copia del estudio mediante el cual se estableció la factibilidad de permitir el tratamiento de datos de ciudadanos colombianos por empresas norteamericanas ubicadas en territorio de los Estados Unidos.
8. ¿Qué autoridad o autoridades de los Estados Unidos son las responsables de proteger los datos personales privados, semiprivados, sensibles y de menores de edad (no solo los datos para fines comerciales)?
9. ¿El Gobierno colombiano ha verificado si frente a dicha (s) entidad (es) un colombiano puede desde Colombia adelantar un trámite de protección de datos frente a las mismas? ¿En caso de existir dicho trámite, cuál es el costo para el ciudadano colombiano y cuando tiempo demoran en responder su petición o requerimiento? ¿Esos trámites, en caso que existan, puede hacerlos

una persona directamente desde Colombia o es necesario contar con un representante judicial y estar ubicado en los Estados Unidos?

10. El artículo 26 de la Ley 1581 de 2012 ordena que los estándares fijados por la Superintendencia de Industria y Comercio sobre nivel adecuado de protección de datos, ***"en ningún caso podrán ser inferiores"*** a los que exige la Ley 1581 de 2012 a sus destinatarios. Así las cosas, de qué manera el Gobierno nacional verificó que la regulación e instituciones de los Estados Unidos tienen un nivel igual o superior al que exige la Ley 1581 de 2012? En particular, responder lo siguiente:

a) En qué normas de los Estados Unidos se hace referencia a todos los derechos que exige el artículo 8° de la Ley 1581 de 2012 respecto de todo tipo de dato *personal-privado*, *sensible, semiprivado y de los menores de edad*. ¿En los Estados Unidos se garantizan los mismos derechos que en Colombia?

b) En qué normas de los Estados Unidos se hace referencia a todos las obligaciones que deben cumplir los Responsables del Tratamiento que exige el artículo 17 de la Ley 1581 de 2012 respecto de todo tipo de dato *personal-privado*, *sensible, semiprivado y de los menores de edad*. ¿En los Estados Unidos se exigen a los Responsables las mismas obligaciones que en Colombia?

c) En qué normas de los Estados Unidos se hace referencia a todos las obligaciones que deben cumplir los Encargados del Tratamiento que exige el artículo 17 de la Ley 1581 de 2012 respecto de todo tipo de dato *personal-privado*, *sensible, semiprivado y de los menores de edad*. ¿En los Estados Unidos se exigen a los Encargados las mismas obligaciones que en Colombia?

d) En qué normas de los Estados Unidos se hace referencia a todos los principios que exige el artículo 4° de la Ley 1581 de 2012 respecto del tratamiento de todo tipo de dato *personal-privado*, *sensible, semiprivado y de los menores de edad*. ¿En los Estados Unidos rigen los mismos principios para el tratamiento de datos que exige la Ley 1581 de 2012?

11. Con relación a la Circular 005 del 10 de agosto de 2017 **emitida** por la Superintendencia de Industria y Comercio ¿Pueden las autoridades colombianas adelantar investigaciones o gestiones, de oficio o a petición de parte, con miras a exigir el respeto del derecho fundamental al hábeas data y a la protección de los datos personales que sean tratados por personas ubicadas o domiciliadas fuera del territorio de la República de Colombia? En caso afirmativo ¿Cuál es el alcance de dicha intervención?
12. ¿En caso de que una persona natural o jurídica ubicada o con domicilio fuera del territorio colombiano se extralimite o afecte el derecho fundamental al hábeas data y a la protección de los datos personales la Superintendencia de Industria y Comercio u otra autoridad nacional puede imponer alguna sanción? De ser así ¿de qué tipo sería la sanción?
13. Qué otro país del mundo ha declarado a los Estados Unidos como un país con nivel adecuado de protección de datos en los mismos términos que lo hizo la SIC mediante la precitada Circular 5 de 2017?
14. ¿Cuáles serían las medidas concretas que dispondría el gobierno de los Estados Unidos en favor de los colombianos en materia de protección de datos?
15. ¿Sírvase informar cuántas denuncias o quejas se han interpuesto en los últimos cinco años contra empresas o personas extrajeras relacionadas con violaciones al derecho fundamental al hábeas data y a la protección de los datos personales? ¿Se han iniciado investigaciones por tales hechos? En caso afirmativo ¿cuáles han sido los resultados de esas investigaciones?
16. En caso de contar con datos estadísticos de percepción ciudadana en materia de protección de datos frente a empresas de origen extranjero sírvase remitir copia de los mismos.
17. ¿La Superintendencia de Industria y Comercio analizó los efectos que tiene la Executive Order: Enhancing Public Safety in the Interior of the United States del 25 de enero de 2017 sobre los datos de los colombianos y las colombianas que se exporten a los Estados Unidos? En caso positivo, por favor remitirnos el estudio o prueba respectiva.
18. ¿La Superintendencia de Industria y Comercio analizó los efectos que tiene la Circular 5 de 2017 -*al incluir a los Estados Unidos como país con nivel adecuado*- frente a una solicitud del Estado colombiano frente a las autoridades europeas con miras a que Europa declare a Colombia como un país que tienen nivel adecuado de protección de datos? En caso positivo, por

favor anexar el estudio respectivo o prueba pertinente.

19. ¿Al incluir a los Estados Unidos como país con nivel adecuado de protección de datos, ello significa que las transferencias de datos -privado, *sensible, semiprivado y de los menores de edad*- desde Colombia a los Estados Unidos no requerirá de la autorización previa, expresa e informada que sí exige la Ley 1581 para transferir datos entre responsables del tratamiento ubicados en territorio colombiano? ¿En otras palabras, según la circular, no se requerirá autorización del titular para enviar sus datos a USA, pero sí cuando los mismos los envíe una empresa domiciliada en Colombia a otra organización ubicada en territorio colombiano?
20. La Superintendencia de Industria y Comercio menciona en la exposición de motivos de la Circular 5 un estudio de 2013 sobre transferencias internacionales de datos que realizó una firma de abogados y en el cual se incluyó a los Estados Unidos como un país con nivel adecuado de protección de datos. Sobre dicho estudio, por favor remitirnos una copia del mismo y responder lo siguiente:

a) ¿Qué firma de abogados realizó dicho estudio?
b) ¿Qué abogado o abogada realizó el estudio y cuál era su experiencia a 2012 respecto de transferencias internacionales de datos?
c) ¿De qué manera la SIC constató o verificó la experiencia especializada de las personas que realizaron el estudio? Por favor remitirnos las hojas de vida que analizó la SIC en 2013 para verificar la experiencia especializada del autor (a) del estudio.
d) ¿La firma de abogados contratada ha tenido o tiene clientes que sean empresas ubicadas en los Estados Unidos?
e) ¿Si ese estudio existía antes de expedirse el primer proyecto de circular en el cual la SIC no incluyó a los Estados Unidos dentro del listado de países con nivel adecuado de protección de datos, por qué razón la SIC cambió radicalmente su posición y en la segunda versión del proyecto de circular sí decidió incluir a los Estados Unidos en dicho listado?

21. Teniendo en cuenta lo que dice el parágrafo primero del numeral 3.2 de la Circular respecto del principio de responsabilidad demostrada, por favor responder lo siguiente:

a) ¿Cuáles son las medidas efectivas y apropiadas que debe adoptar el Responsable de tratamiento de datos para garantizar en los Estados Unidos el adecuado tratamiento de los datos personales que son exportados desde Colombia a dicho país?
b) ¿Esas medidas son suficientes para dar plena certeza al ciudadano colombianos que sus datos serán tratados debidamente en los Estados Unidos y que sus derechos serán plenamente respetados en dicho país? Por favor explicar su respuesta en caso que sea afirmativa.
c) ¿Por qué la SIC no menciona en la circular las medidas concretas que se deben adoptar en virtud del principio de responsabilidad demostrada y deja el tema en manos de cada Responsables del tratamiento?
d) ¿No cree la SIC que la ausencia de dichas medidas en la circular dejará al arbitrio de cada Responsable el nivel de protección y garantía de los derechos de los titulares de los datos que son exportados desde Colombia a los Estados Unidos?

22. Teniendo en cuenta lo que dice el parágrafo segundo del numeral 3.2 de la Circular, por favor responder lo siguiente:

a) ¿Una empresa que exportara datos desde Colombia a otro país puede, por sí misma y sin intervención de la SIC, determinar si ese país cumple los estándares fijados en el numeral 3.1 de la circular?
b) ¿Si ello es así, la SIC no está transfiriendo sus obligaciones legales a los particulares Responsable del tratamiento que desean exporta datos de colombianos?

23. ¿Qué quiere decir el parágrafo cuarto del numeral 3.2 de la Circular? Significa que la SIC vía circular deroga la necesidad de que exista un contrato de transmisión internacional de datos previsto en el artículo 25 de Decreto 1377 de 2013? ¿Por qué razón la SIC mediante la Circular equipara las transferencias con las transmisiones internacionales?
24. ¿Qué significa en concreto el parágrafo del numeral 3.3 de la Circular Externa 5 del 10 de agosto de 2017?
25. ¿La Superintendencia de Industria y Comercio contrató algún asesor externo para redactar la Circular 5 de 2017? En caso positivo:

a) ¿De qué manera la SIC constató o verificó la experiencia especializada en transferencias internacionales de la persona contratada? Por favor remitirnos la hoja de vida que analizó la SIC para contratar dicha persona.

b) ¿La persona o firma contratada ha tenido o tiene clientes que sean empresas ubicadas en los Estados Unidos?

c) La persona o firma contratada ha tenido o tiene clientes que se dediquen a ofrecer servicios relacionados con el principio de responsabilidad demostrada o accountability?

De los honorables Senadores,

IV

Consideración y votación de proyectos en primer debate

1. **Proyecto de ley número 89 de 2017 Senado,** *por medio de la cual se modifica la Ley Estatutaria 1581 de 2012*.

Autor: Honorable Senador *Jaime Amín Hernández.*

Ponente primer debate: Honorable Senador *Jaime Amín Hernández*.

Publicación:

Proyecto original: ***Gaceta del Congreso*** número 713 de 2017.

Ponencia primer debate: ***Gaceta del Congreso*** número 772 de 2017.

2. **Proyecto de ley número 30 de 2017 Senado,** *por medio de la cual se modifica el Decreto-ley 888 de 2017*.

Autores: Honorables Senadores *Paloma Valencia Laserna, Jaime Amín Hernández, Alfredo Rangel Suárez, Carlos Felipe Mejía Mejía*.

Ponente primer debate: Honorable Senador *Jaime Amín Hernández.*

Publicación:

Proyecto original: ***Gaceta del Congreso*** número 629 de 2017.

Ponencia primer debate Senado: ***Gaceta del Congreso*** número 717 de 2017.

3. **Proyecto de ley número 29 de 2017 Senado,** *por medio de la cual se deroga el Decreto-ley 898 de 2017*.

Autores: Honorables Senadores *Paloma Valencia Laserna, Jaime Amín Hernández, Daniel Cabrales Castillo, Alfredo Rangel Suárez, Carlos Felipe Mejía Mejía*.

Ponente primer debate: Honorable Senador *Paloma Valencia Laserna.*

Publicación:

Proyecto original: ***Gaceta del Congreso*** número 629 de 2017.

Ponencia primer debate: ***Gaceta del Congreso*** número 717 de 2017.

4. **Proyecto de ley número 20 de 2017 Senado,** *por medio de la cual se reforma el Decreto 1421 de 1993 en relación con la remuneración de los Alcaldes Locales y los Ediles de Bogotá*.

Autor: Honorable Senador *Roy Leonardo Barreras Montealegre.*

Ponente primer debate: Honorable Senador *Roy Barreras Montealegre.*

Publicación:

Proyecto original: ***Gaceta del Congreso*** número 601 de 2017.

Ponencia primer debate: ***Gaceta del Congreso*** número 760 de 2017.

5. **Proyecto de ley número 34 de 2017 Senado,** *por medio del cual se fortalece el ejercicio funcional de las Personerías Municipales*.

Autor: Honorable Senador *Roy Barreras Montealegre.*

Ponente primer debate: Honorable Senador *Roy Barreras Montealegre.*

Publicación:

Proyecto original: ***Gaceta del Congreso*** número 667 de 2017.

Ponencia primer debate: ***Gaceta del Congreso*** número 760 de 2017.

6. **Proyecto de ley número 32 de 2017 Senado,** *por medio del cual se modifica el Decreto 903 del 29 de mayo de 2017 y se dictan otras disposiciones.*

Autores: Honorables Senadores *Jaime Amín Hernández, Daniel Cabrales Castillo, Alfredo Rangel Suárez, Carlos Felipe Mejía Mejía, Paloma Valencia Laserna*.

Ponente primer debate: Honorable Senador *Alfredo Rangel Suárez.*

Publicación:

Proyecto original: ***Gaceta del Congreso*** número 629 de 2017.

Ponencia primer debate: ***Gaceta del Congreso*** número 748 de 2017.

7. **Proyecto de Acto Legislativo número 03 de 2017 Senado,** *por medio del cual se reforma la Constitución Política de Colombia en lo relativo a la remuneración de los miembros del Congreso de la República*.

Autores: Honorables Senadores *Álvaro Uribe Vélez, Paola Holguín Moreno, Daniel Cabrales Castillo, Jaime Amín Hernández, Thania Vega de Plazas, Honorio Henríquez Pinedo, Alfredo Rangel Suárez, Nohora Tovar Rey, Susana Correa Borrero, Alfredo Ramos Maya; honorables Representantes Óscar Darío Pérez, Pierre Eugenio García, Hugo Hernán González.*

Ponente primer debate: Honorable Senador *Alfredo Rangel Suárez.*

Publicación:

Proyecto original: ***Gaceta del Congreso*** número 582 de 2017.

Ponencia primer debate: ***Gaceta del Congreso*** número 746 de 2017.

V

Lo que propongan los honorables Senadores

VI

Anuncio de proyectos

VII

Negocios sustanciados por la Presidencia

El Presidente,

Honorable Senador *Roosvelt Rodríguez Rengifo.*

El Vicepresidente,

Honorable Senador *Horacio Serpa Uribe.*

El Secretario General,

Guillermo León Giraldo Gil.

La Presidencia abre la discusión del Orden del Día e informa que una vez se constituya quórum decisorio se someterá a votación.

Atendiendo instrucciones de la Presidencia por Secretaría se da lectura al siguiente punto del Orden del Día:

II

Consideración y aprobación de actas

Acta número 06 del 15 de agosto de 2017, *Gaceta del Congreso* número 756 de 2017; Acta número 07 del 16 de agosto de 2017, *Gaceta del Congreso* número 757 de 2017; Acta número 08 del 22 de agosto de 2017, *Gaceta del Congreso* número 776 de 2017; Acta número 09 del 23 de agosto de 2017, *Gaceta del Congreso* número 768 de 2017; Acta número 10 del 29 de agosto de 2017; Acta número 11 del 30 de agosto de 2017; Acta número 12 del 12 de septiembre de 2017

La Presidencia abre la discusión del **Acta número 06 del 15 de agosto de 2017, publicada en la *Gaceta del Congreso* número 756 de 2017; Acta número 07 del 16 de agosto de 2017, publicada en la *Gaceta del Congreso* número 757 de 2017, Acta número 08 del 22 de agosto de 2017 publicada en la *Gaceta del Congreso* número 776 de 2017; Acta número 09 del 23 de agosto de 2017 publicada en la *Gaceta del Congreso* número 768 de 2017** e informa que una vez se constituya quórum decisorio se someterá a votación.

Atendiendo instrucciones de la Presidencia por Secretaria se da lectura al siguiente punto del Orden del Día:

III

Citación a los señores Ministros del Despacho y altos funcionarios del Estado

Proposición número 08

En atención a lo previsto en la Circular Externa 005 del 10 de agosto de 2017 y propendiendo por la garantía del derecho fundamental al hábeas data y a la protección de los datos personales de los colombianos en materia de recolección, almacenamiento, uso, circulación y en general cualquier tipo de operaciones efectuadas por empresas norteamericanas, se hace necesario, urgente e impostergable, que de manera inmediata se cite a debate de control político al Ministro de Tecnologías de la Información y las Comunicaciones, doctor David Luna; a la Ministra de Comercio Industria y Turismo, doctora María Lorena Gutiérrez Botero, al Superintendente de Industria y Comercio, doctor Pablo Felipe Robledo y a la Superintendente Delegada para la Protección de Datos, doctora María Claudia Cabiedes Mejía para que respondan por el cuestionario que se anexa.

También invítese al Director del Observatorio Ciro Angarita Barón de Protección de Datos y del GECTI -Grupo de Estudios en Internet, Comercio electrónico, Telecomunicaciones e Informática- de la Universidad de los Andes, doctor Nelson Remolina Angarita; al Director de ACUI, doctor Antonio Medina Gómez; a los representantes de Google Colombia, Microsoft Colombia y Twitter Colombia.

Adicionalmente, le solicito respetuosamente que para este debate se tenga transmisión en vivo del canal institucional del Congreso de la república y demás medios de comunicación con que la corporación cuente.

De los honorables Senadores,

Jaime Amín Hernández,

Senador de la República

CUESTIONARIO:

1. ¿Existe tratado o convenio vigente y jurídicamente vinculante entre Estados Unidos y Colombia para el tratamiento de datos personales?
2. ¿Existe tratado o convenio vigente y jurídicamente vinculante entre algún otro país y Colombia para el tratamiento de datos personales? En caso afirmativo ¿cuáles son los derechos en cabeza de los titulares de la información, así como los procedimientos y sanciones previstos para proteger el derecho fundamental al hábeas data y a la protección de datos personales?
3. ¿Actualmente algún país extranjero cuenta con autorización para el tratamiento de datos de colombianos? En caso afirmativo informar reglamentación que rige la transferencia internacional de datos para cada caso.
4. En materia de reciprocidad, ¿Existe algún documento de las autoridades de los Estados Unidos que declaren formalmente a Colombia como un país que tenga nivel adecuado de protección de datos? ¿Existe algún documento de las autoridades de los

Estados Unidos que permita que personas naturales o jurídicas ubicadas en territorio colombiano puedan receptar y tratar datos de ciudadanos americanos? De ser así ¿cuáles son las condiciones que deben reunir las personas naturales o jurídicas ubicadas en territorio colombiano para efectuar tratamiento de datos de norteamericanos? Sírvase efectuar análisis comparado entre la regulación a la cual deben someterse los Responsables del Tratamiento de Datos colombianos y las condiciones a las que estarían sujetas las personas naturales o jurídicas americanas Responsables del Tratamiento de Datos.

5. ¿Cómo se ha manejado hasta ahora la recolección, almacenamiento, uso, circulación y en general cualquier tipo de operaciones efectuadas por empresas norteamericanas y que involucran datos de connacionales?
6. Sírvase informar cuáles personas naturales o jurídicas de los Estados Unidos actualmente tratan datos de colombianos, indicando el volumen de información que recolectan, almacenan, usan o circulan.
7. Sírvase remitir copia del estudio mediante el cual se estableció la factibilidad de permitir el tratamiento de datos de ciudadanos colombianos por empresas norteamericanas ubicadas en territorio de los Estados Unidos.
8. ¿Qué autoridad o autoridades de los Estados Unidos son las responsables de proteger los datos personales privados, semiprivados, sensibles y de menores de edad (no solo los datos para fines comerciales)?
9. ¿El Gobierno colombiano ha verificado si frente a dicha (s) entidad (es) un colombiano puede desde Colombia adelantar un trámite de protección de datos frente a las mismas? ¿En caso de existir dicho trámite, cuál es el costo para el ciudadano colombiano y cuando tiempo demoran en responder su petición o requerimiento? ¿Esos trámites, en caso que existan, puede hacerlos una persona directamente desde Colombia o es necesario contar con un representante judicial y estar ubicado en los Estados Unidos?
10. El artículo 26 de la Ley 1581 de 2012 ordena que los estándares fijados por la Superintendencia de Industria y Comercio sobre nivel adecuado de protección de datos, ***"en ningún caso podrán ser inferiores"*** a los que exige la Ley 1581 de 2012 a sus destinatarios. Así las cosas, de qué manera el Gobierno nacional verificó que la regulación e instituciones de los Estados Unidos tiene un nivel igual o superior al que exige la Ley 1581 de 2012? En particular, responder lo siguiente:

a) En qué normas de los Estados Unidos se hace referencia a todos los derechos que exige el artículo 8° de la Ley 1581 de 2012 respecto de todo tipo de dato *personal-privado*, *sensible, semiprivado y de los menores de edad*. ¿En los Estados Unidos se garantizan los mismos derechos que en Colombia?
b) En qué normas de los Estados Unidos se hace referencia a todos las obligaciones que deben cumplir los Responsables del Tratamiento que exige el artículo 17 de la Ley 1581 de 2012 respecto de todo tipo de dato *personal-privado*, *sensible, semiprivado y de los menores de edad*. ¿En los Estados Unidos se exigen a los Responsables las mismas obligaciones que en Colombia?
c) En qué normas de los Estados Unidos se hace referencia a todos las obligaciones que deben cumplir los Encargados del Tratamiento que exige el artículo 17 de la Ley 1581 de 2012 respecto de todo tipo de dato *personal-privado*, *sensible, semiprivado y de los menores de edad*. ¿En los Estados Unidos se exigen a los Encargados las mismas obligaciones que en Colombia?
d) En qué normas de los Estados Unidos se hace referencia a todos los principios que exige el artículo 4° de la Ley 1581 de 2012 respecto del tratamiento de todo tipo de dato *personal-privado*, *sensible, semiprivado y de los menores de edad*. ¿En los Estados Unidos rigen los mismos principios para el tratamiento de datos que exige la Ley 1581 de 2012?

11. Con relación a la Circular 005 del 10 de agosto de 2017 emitida por la Superintendencia de Industria y Comercio ¿Pueden las autoridades colombianas adelantar investigaciones o gestiones, de oficio o a petición de parte, con miras a exigir el respeto del derecho fundamental al hábeas data y a la protección de los datos personales que sean tratados por personas ubicadas o domiciliadas fuera del territorio de la República de Colombia? En caso afirmativo ¿Cuál es el alcance de dicha intervención?
12. ¿En caso de que una persona natural o jurídica ubicada o con domicilio fuera del territorio colombiano se extralimite o afecte el derecho fundamental al hábeas data y a la protección de los datos personales la Superintendencia de Industria y Comercio u

otra autoridad nacional puede imponer alguna sanción? De ser así ¿de qué tipo sería la sanción?

13. Qué otro país del mundo ha declarado a los Estados Unidos como un país con nivel adecuado de protección de datos en los mismos términos que lo hizo la SIC mediante la precitada Circular 5 de 2017?
14. ¿Cuáles serían las medidas concretas que dispondría el gobierno de los Estados Unidos en favor de los colombianos en materia de protección de datos?
15. ¿Sírvase informar cuántas denuncias o quejas se han interpuesto en los últimos cinco años contra empresas o personas extrajeras relacionadas con violaciones al derecho fundamental al hábeas data y a la protección de los datos personales? ¿Se han iniciado investigaciones por tales hechos? En caso afirmativo ¿cuáles han sido los resultados de esas investigaciones?
16. En caso de contar con datos estadísticos de percepción ciudadana en materia de protección de datos frente a empresas de origen extranjero sírvase remitir copia de los mismos.
17. ¿La Superintendencia de Industria y Comercio analizó los efectos que tiene la Executive Order: Enhancing Public Safety in the Interior of the United States del 25 de enero de 2017 sobre los datos de los colombianos y las colombianas que se exporten a los Estados Unidos? En caso positivo, por favor remitirnos el estudio o prueba respectiva.
18. ¿La Superintendencia de Industria y Comercio analizó los efectos que tiene la Circular 5 de 2017 -*al incluir a los Estados Unidos como país con nivel adecuado*- frente a una solicitud del Estado colombiano frente a las autoridades europeas con miras a que Europa declare a Colombia como un país que tienen nivel adecuado de protección de datos? En caso positivo, por favor anexar el estudio respectivo o prueba pertinente.
19. ¿Al incluir a los Estados Unidos como país con nivel adecuado de protección de datos, ello significa que las transferencias de datos -privado, *sensible, semiprivado y de los menores de edad*- desde Colombia a los Estados Unidos no requerirá de la autorización previa, expresa e informada que sí exige la Ley 1581 para transferir datos entre responsables del tratamiento ubicados en territorio colombiano? ¿En otras palabras, según la circular, no se requerirá autorización del titular para enviar sus datos a USA, pero sí cuando los mismos los envíe una empresa domiciliada en Colombia a otra organización ubicada en territorio colombiano?
20. La Superintendencia de Industria y Comercio menciona en la exposición de motivos de la Circular 5 un estudio de 2013 sobre transferencias internacionales de datos que realizó una firma de abogados y en el cual se incluyó a los Estados Unidos como un país con nivel adecuado de protección de datos. Sobre dicho estudio, por favor remitirnos una copia del mismo y responder lo siguiente:

a) ¿Qué firma de abogados realizó dicho estudio?
b) ¿Qué abogado o abogada realizó el estudio y cuál era su experiencia a 2012 respecto de transferencias internacionales de datos?
c) ¿De qué manera la SIC constató o verificó la experiencia especializada de las personas que realizaron el estudio? Por favor remitirnos las hojas de vida que analizó la SIC en 2013 para verificar la experiencia especializada del autor (a) del estudio.
d) ¿La firma de abogados contratada ha tenido o tiene clientes que sean empresas ubicadas en los Estados Unidos?
e) ¿Si ese estudio existía antes de expedirse el primer proyecto de circular en el cual la SIC no incluyó a los Estados Unidos dentro del listado de países con nivel adecuado de protección de datos, por qué razón la SIC cambió radicalmente su posición y en la segunda versión del proyecto de circular sí decidió incluir a los Estados Unidos en dicho listado?

21. Teniendo en cuenta lo que dice el parágrafo primero del numeral 3.2 de la Circular respecto del principio de responsabilidad demostrada, por favor responder lo siguiente:

a) ¿Cuáles son las medidas efectivas y apropiadas que debe adoptar el Responsable de tratamiento de datos para garantizar en los Estados Unidos el adecuado tratamiento de los datos personales que son exportados desde Colombia a dicho país?
b) ¿Esas medidas son suficientes para dar plena certeza al ciudadano colombianos que sus datos serán tratados debidamente en los Estados Unidos y que sus derechos serán plenamente respetados en dicho país? Por favor explicar su respuesta en caso que sea afirmativa.
c) ¿Por qué la SIC no menciona en la circular las medidas concretas que se deben adop-

tar en virtud del principio de responsabilidad demostrada y deja el tema en manos de cada Responsables del tratamiento?

d) ¿No cree la SIC que la ausencia de dichas medidas en la circular dejará al arbitrio de cada Responsable el nivel de protección y garantía de los derechos de los titulares de los datos que son exportados desde Colombia a los Estados Unidos?

22. Teniendo en cuenta lo que dice el parágrafo segundo del numeral 3.2 de la Circular, por favor responder lo siguiente:

a) ¿Una empresa que exportará datos desde Colombia a otro país puede, por sí misma y sin intervención de la SIC, determinar si ese país cumple los estándares fijados en el numeral 3.1 de la circular?

b) ¿Si ello es así, la SIC no está transfiriendo sus obligaciones legales a los particulares Responsable del tratamiento que desean exporta datos de colombianos?

23. ¿Qué quiere decir el parágrafo cuarto del numeral 3.2 de la Circular? Significa que la SIC vía circular deroga la necesidad de que exista un contrato de transmisión internacional de datos previsto en el artículo 25 de Decreto 1377 de 2013? ¿Por qué razón la SIC mediante la Circular equipara las transferencias con las transmisiones internacionales?

24. ¿Qué significa en concreto el parágrafo del numeral 3.3 de la Circular Externa 5 del 10 de agosto de 2017?

25. ¿La Superintendencia de Industria y Comercio contrató algún asesor externo para redactar la Circular 5 de 2017? En caso positivo:

a) ¿De qué manera la SIC constató o verificó la experiencia especializada en transferencias internacionales de la persona contratada? Por favor remitirnos la hoja de vida que analizó la SIC para contratar dicha persona.

b) ¿La persona o firma contratada ha tenido o tiene clientes que sean empresas ubicadas en los Estados Unidos?

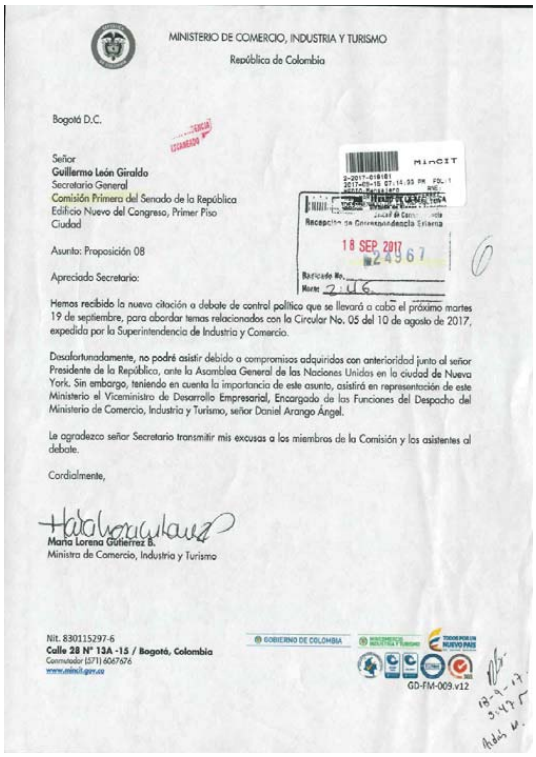
c) La persona o firma contratada ha tenido o tiene clientes que se dediquen a ofrecer servicios relacionados con el principio de responsabilidad demostrada o accountability?

De los honorables Senadores,

Jaime Amín Hernández,

Senador de la República

La Secretaría informa de los citados e invitados: el doctor David Luna Sánchez - Ministro de Tecnologías de la Información y las Comunicaciones, se encuentra presente; la doctora María Lorena Gutiérrez Botero - Ministra de Comercio Industria y Turismo, se excusó y delega al doctor Daniel Arango Ángel – Viceministro de Desarrollo del Ministerio de Comercio, Industria y Turismo, no se ha hecho presente; el doctor Pablo Felipe Robledo - Superintendente de Industria y Comercio, se encuentra presente; la doctora María Claudia Cabiedes Mejía - Superintendente Delegada para la Protección de Datos, se encuentra presente; y de los Invitados: al doctor Nelson Remolina Angarita - Director de Observatorio Ciro Angarita Barón sobre la protección de datos personales en Colombia. Director del GECTI Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática- de la Universidad de los Andes, se encuentra presente; el doctor Antonio Medina Gómez - Director de ACUI, se encuentra presente; la doctora Ana Lucía Lenis – representante de Google, no se encuentra presente; el doctor Andrés Umaña Chaux – Representante de Microsoft, se encuentra presente; el doctor Diego Santos – Representante en Colombia de Twitter, no se encuentra presente; el doctor Alberto Samuel Yohai – Presidente ejecutivo de la Cámara Colombiana de Informática y Telecomunicaciones, se excusa delega a la doctora Sandra Pascua - vicepresidenta de la Cámara Colombiana de Informática y Telecomunicaciones, aún no se ha hecho presente; el doctor Carlos Alfonso Negret Mosquera – Defensor del Pueblo se excusa; el doctor Fernando Carrillo Flórez – Procurador General de la Nación se excusó y delega a unos funcionarios como observadores, se encuentra presente el citante honorable Senador Jaime Amín Hernández.



MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
República de Colombia

Bogotá D.C.

Señor
Guillermo León Giraldo
Secretario General
Comisión Primera del Senado de la República
Edificio Nuevo del Congreso, Primer Piso
Ciudad

MINCIT
18 SEP. 2017
24967

Asunto: Proposición 08

Apreciado Secretario:

Hemos recibido la nueva citación a debate de control político que se llevará a cabo el próximo martes 19 de septiembre, para abordar temas relacionados con la Circular No. 05 del 10 de agosto de 2017, expedida por la Superintendencia de Industria y Comercio.

Desafortunadamente, no podré asistir debido a compromisos adquiridos con anterioridad junto al señor Presidente de la República, ante la Asamblea General de las Naciones Unidas en la ciudad de Nueva York. Sin embargo, teniendo en cuenta la importancia de este asunto, asistirá en representación de este Ministerio el Viceministro de Desarrollo Empresarial, Encargado de las Funciones del Despacho del Ministerio de Comercio, Industria y Turismo, señor Daniel Arango Angel.

Le agradezco señor Secretario transmitir mis excusas a los miembros de la Comisión y los asistentes al debate.

Cordialmente,

María Lorena Gutiérrez B.
Ministra de Comercio, Industria y Turismo

Nit. 830115297-6
Calle 28 N° 13A -15 / Bogotá, Colombia
Conmutador (571) 6067676
www.mincit.gov.co

GOBIERNO DE COLOMBIA

GD-FM-009.v12

PROCURADURIA GENERAL DE LA NACION

Bogotá D.C., 18 SEP 2017

S.P. 3579

Doctor
GUILLERMO LEÓN GIRALDO GIL
Secretario General Comisión Primera Senado
Congreso de la República
Ciudad

Asunto: Debate control político día 19 de septiembre

Siguiendo instrucciones impartidas por el señor Procurador General de la Nación, doctor Fernando Carrillo Flórez, me permito informarle que él no podrá asistir el día 19 de septiembre, al debate control político relacionado con la proposición 08, telecomunicaciones e informática, por encontrarse cumpliendo compromisos previamente adquiridos como Jefe del Ministerio Público.

No obstante y dada la importancia del tema asistirá en calidad de observador el doctor **Gerardo Alfonso Dallos Jabbour**, identificado con cédula de ciudadanía 80.423.442, funcionario adscrito a la Procuraduría Delegada para la Vigilancia Preventiva de la Función Pública.

Cordial saludo,

JÚBER DARIO ARIZA RUEDA
Secretario Privado

Copia: Procuraduría Delegada para la Vigilancia Preventiva de la Función Pública.

Proyectó: Ma. Elsa
E-2017-783387

19 Sep 2017
11:40 Am

Gmail

Comisión Primera Senado de la República de Colombia
<comisionprimera@gmail.com>

EXCUSA CCIT Y DELEGACIÓN PARA PARTICIPACION EN DEBATE PROPOSICIÓN NO. 08

Sandra Pascua <sandra.pascua@ccit.org.co> 19 de septiembre de 2017, 8:36
Para: comisionprimera@gmail.com

Buenos dia doctor Giraldo:

Adjunto estoy enviando carta suscrita por el doctor Alberto Samuel Yohai, Presidente Ejecutivo de la CCIT, en la cual agradece la invitación al debate a que hace referencia la Proposición No. 08 que se llevará cabo en esa Comisión el día de hoy, se excusa por no poder asistir al mismo y delega en mí su participación en representación de la CCIT.

Agradeciéndole la atención a la presente, me suscribo de usted con sentimientos de consideración y aprecio.

Cordialmente,

CCIT
CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES

SANDRA PASCUA
Vicepresidente
Cámara Colombiana de Informática y Telecomunicaciones - CCIT
sandra.pascua@ccit.org.co
+ 571 756-3456
Carrera 11A #93-67 Of. 401
Bogotá, Colombia
www.ccit.org.co

Carta CCIT_Delegación_Debate_Datos Personales.pdf
601K

CCIT Cámara Colombiana de Informática y Telecomunicaciones

Bogotá D.C., Septiembre 19 de 2017

Doctor
GUILLERMO LEON GIRALDO GIL
Secretario General Comisión Primera
H. SENADO DE LA REPÚBLICA
Ciudad

Asunto: Invitación Proposición No. 08

Apreciado Guillermo:

En primero lugar agradezco la amable invitación que por su conducto me hace el Honorable Senador Roosvelt Rodríguez Rengifo, Presidente de esa célula legislativa, al debate a que hace referencia la Proposición No. 08, firmada por los Honorables Senadores Jaime Amín Hernández, Alfredo Rangel Suarez y Paloma Valencia Laserna, que se llevara a cabo el día martes 19 de septiembre de 2017, en el Salón Guillermo Valencia del Capitolio Nacional.

Lastimosamente por conflictos de agenda no me será posible asistir al mismo, por tal razón he delegado mi participación en la señora Sandra Pascua, Vicepresidente de la CCIT.

De antemano agradezco su atención a la presente.

Cordialmente,

ALBERTO SAMUEL YOHAI
Presidente Ejecutivo
Cámara Colombiana de Informática y Telecomunicaciones – CCIT

PROCURADURIA GENERAL DE LA NACION

Bogotá D.C., 18 SEP 2017

S.P. 3579

Doctor
GUILLERMO LEÓN GIRALDO GIL
Secretario General Comisión Primera Senado
Congreso de la República
Ciudad

Asunto: Debate control político día 19 de septiembre

Siguiendo instrucciones impartidas por el señor Procurador General de la Nación, doctor Fernando Carrillo Flórez, me permito informarle que él no podrá asistir el día 19 de septiembre, al debate control político relacionado con la proposición 08, telecomunicaciones e informática, por encontrarse cumpliendo compromisos previamente adquiridos como Jefe del Ministerio Público.

No obstante y dada la importancia del tema asistirá en calidad de observador el doctor **Gerardo Alfonso Dallos Jabbour**, identificado con cédula de ciudadanía 80.423.442, funcionario adscrito a la Procuraduría Delegada para la Vigilancia Preventiva de la Función Pública.

Cordial saludo,

JÚBER DARIO ARIZA RUEDA
Secretario Privado

Copia: Procuraduría Delegada para la Vigilancia Preventiva de la Función Pública.

Proyectó: Ma. Elsa
E-2017-783387

Defensoria del Pueblo
COLOMBIA

Bogotá D.C. 15 SEP 2017

Doctor
GUILLERMO LEÓN GIRALDO GIL
Secretario General
Comisión Primera
SENADO DE LA REPÚBLICA
Edificio Nuevo del Congreso - Primer Piso
comisionprimera@gmail.com
BOGOTÁ, D.C.

SENADO DE LA REPÚBLICA
Unidad de Correspondencia
Recepción de Correspondencia Externa
15 SEP 2017
Radicado No. 24826
Hora: 9:19

Referencia: Respuesta invitación oficio CPR-CS-0668-2017- Delegación

Respetado doctor León:

Agradezco la invitación a la sesión de la comisión para desarrollar la Proposición No. 08 sobre "**El Derecho fundamental al habeas data y a la protección de los datos personales de los colombianos en materia de recolección, almacenamiento, uso, circulación y en general cualquier tipo de operaciones efectuadas por empresas norteamericanas**", que se llevará a cabo el martes 19 de septiembre de 2017, a las 10:00 a.m, en las instalaciones del salón Guillermo Valencia del Capitolio Nacional.

Extiendo las debidas excusas, pues no podré asistir por compromisos en el exterior previamente adquiridos y de carácter indelegable.

Por último, hago propicia la ocasión para reiterarte los sentimientos de mi más alta consideración.

Cordialmente,

CARLOS ALFONSO NEGRET MOSQUERA
Defensor del Pueblo

Copia: Dra. Paula Robledo
Anexos: N/A
Proyectó: Lina Rodríguez
Revisó: José María Balcázar
Archivado en: Oficios Enviados
Consecutivo Dependencia:

01287

Carrera 9 No. 16 - 21
PBX: (57) 1 3144000 - Línea Nacional: 01 8000 914814
www.defensoria.gov.co

PROCURADURIA GENERAL DE LA NACION

Bogotá D.C., 18 SEP 2017

S.P. 3579

SENADO DE LA REPÚBLICA
Unidad de Correspondencia
Recepción de Correspondencia Externa
19 SEP 2017
Radicado No. 25083
Hora: 10:10

Doctor
GUILLERMO LEÓN GIRALDO GIL
Secretario General Comisión Primera Senado
Congreso de la República
Ciudad

Asunto: Debate control político día 19 de septiembre

Siguiendo instrucciones impartidas por el señor Procurador General de la Nación, doctor Fernando Carrillo Flórez, me permito informarle que él no podrá asistir el día 19 de septiembre, al debate control político relacionado con la proposición 08, telecomunicaciones e informática, por encontrarse cumpliendo compromisos previamente adquiridos como Jefe del Ministerio Público.

No obstante y dada la importancia del tema asistirá en calidad de observador el doctor **Gerardo Alfonso Dallos Jabbour**, identificado con cédula de ciudadanía 80.423.442, funcionario adscrito a la Procuraduría Delegada para la Vigilancia Preventiva de la Función Pública.

Cordial saludo,

JÚBER DARIO ARIZA RUEDA
Secretario Privado

Copia: Procuraduría Delegada para la Vigilancia Preventiva de la Función Pública.

Proyectó Ma. Elsa
E-2017-783387

La Presidencia concede el uso de la palabra al citante honorable Senador Jaime Amín Hernández:

Muchas gracias señor Presidente, agradezco la presencia en la Comisión del Ministro Luna, del Superintendente Robledo, de la Superintendente Delegada para Datos la doctora Caviedes, lo mismo de quienes cursamos una invitación para que nos acompañaran en este debate, que nosotros estimamos de la mayor importancia.

Quiero comentar un poco antecedentes de la relación que a mí me ha llevado adentrarme en el tema de la protección de datos de los colombianos, señor Superintendente, en el año 2002 cuando yo fui también Congresista de la Comisión Primera de Cámara, me di cuenta por conversaciones académicas con algunos otros abogados, yo lo soy, que en Colombia la ciudadanía no tenía un nivel adecuado de protección de datos, pese a que el artículo 15 de la Constitución prescribía la protección integral del hábeas data, la protección integral del hábeas data, el buen nombre de los ciudadanos frente al ejercicio de almacenamiento, recolección, tratamiento y circulación de sus datos en los diferentes bancos de datos, sobre todo aquellos de carácter financiero.

Al no haber una regulación legal, había una consagración normativa constitucional, pero no legal, la gente tenía que acudir a la tutela, es así como comenzamos un proceso interesante con el entonces Ministro Carrasquilla, Andrés Flórez de Fogafín, Guillermo Botero de Fenalco, en la ANDI estaba el hoy Ministro de Defensa y algunos otros actores del sector financiero, hablo de Data Crédito, Sifín, Covinoc, que eran como los bancos de datos financieros más relevantes, más conocidos.

En un ejercicio que nos llevó casi 3 años, 3 años de reuniones, 3 años de estudios, de avances, de compartir información entre los actores públicos y privados que tenían que ver con el manejo de la información de los datos de los colombianos, porque el ciudadano colombiano estaba expósito frente a la posición de vida y legal de su buen nombre, solamente la acción de tutela suplía esa falta y esa ausencia de reglamentación y protección para los datos de los colombianos y sacamos entonces la primera de las leyes que regularon el tema del hábeas data en Colombia, la 1266 que después tuvo un desarrollo normativo complementario con la 1581.

Que son las dos normas marco de protección de los datos de los colombianos, del buen nombre de los colombianos y esto fue muy importante señor Presidente, porque Colombia avanzo en la dirección correcta en un patio latinoamericano que veía como muy pocos países, por decir que ninguno, salvo tal vez Argentina, un poco Brasil, otro tanto México, un poquito, regulaban a través de disposiciones la protección adecuada para los ciudadanos al buen nombre.

Creo que es menester hacerle un reconocimiento a quien desde entonces me acompaño en la tratativa de esos temas, el doctor Nelson Remolina que está aquí presente, de la Universidad de los Andes, que sin duda es una autoridad Latinoamericana en el tema.

Creo que ese ejercicio que hice como Representante a la Cámara de sacar una ley que permitiera los actores y sobre todo a los actores y sobre todo a los ciudadanos de a pie contar con una herramienta útil que le quitara ese San Benito y ese suplicio y ese calvario de tener que acudir a la tutela señor Presidente fue un paso adelante enorme, enorme, en la protección de los datos de los colombianos.

Hoy los colombianos tenemos un sistema de protección adecuado, no perfecto, por supuesto, tal vez perfectible en la medida en que haya unas normas complementarias tanto de carácter administrativo del gobierno como del Congreso y ahora me voy a referir a eso, pero sin duda le quito esa diría yo inapropiada suspicacia al ciudadano de que solamente a través de la tutela se podían proteger sus derechos, hoy hay una ley y yo creo que fue un gran paso señor Ministro, no suficiente, pero creo que Colombia dio pasos que la pusieron en la dirección indicada para proteger la información y los datos de sus ciudadanos.

Las leyes en el Congreso tienen que tener y en eso los Congresistas, doctor Manuel Enríquez, tenemos que poner de nuestra parte, nosotros no somos sino instrumentos, para que en la confección de la ley esa norma salga con la mayor utilidad posible.

Por eso a mí en lo personal me gusta discutir con los actores frente a los cuales una norma o un proyecto de ley de mi iniciativa, pueda encontrar consenso, mejoría y por qué no decirlo también un trámite mucho más expedito cuando ya bien confeccionada, bien socializada se ponga a disposición de las comisiones y de las plenarias aquí en el Congreso.

Esto lo digo señor Ministro, porque ahora que tengo el honor de estar acá en esta corporación he venido trabajando también con la Universidad de los Andes otro proyecto de ley que hemos discutido mucho con los actores que tienen que ver con el tema, también tuve la oportunidad de conversarlo con usted señor Ministro y es buscar que todas esas empresas que operan en Colombia, que almacenan datos de colombianos, que recolectan información de colombianos, que distribuyen y por qué no decirlo también, hacen uso de la información de los colombianos, pero que no tienen domicilio en Colombia, puedan someterse a la ley colombiana particularmente a las competencias funcionales de la Superintendencia de Industria y Comercio y los colombianos puedan mejorar su estándar de protección frente al uso de la información que hacen esas empresas.

Muchas han sido las reuniones y aquí están algunos de los actores y representantes de esas empresas, que yo he hecho con Microsoft, con Google, con Twitter, en fin, con una infinidad de empresas asociadas en la Cámara Colombiana de Protección de Datos, lamento que no esté el doctor Yohai, pero entiendo que tendrá algún delegado en este debate, porque la idea es como hacer, como mejorar ese camino de protección en el que ha venido ya Colombia dando unas puntadas muy importantes y que el gobierno y el Congreso encuentren diría yo, un escenario de concertación y no un escenario de confrontación doctor Enríquez Maya.

Porque nosotros nada hacemos con que la Unidad de Protección de Datos en Colombia o el propio Ministerio de las Comunicaciones se opongan a una iniciativa que busque mejorar desde el Congreso la protección de datos de los colombianos, ese tema que lo voy abordar al final del debate, lo dejo solamente como un elemento de discusión ahora que la Superintendencia de Industria y Comercio expidió una circular que a nuestro juicio doctor Robledo pone en entre dicho la seguridad jurídica que debe prevalecer en todo lo que tenga que ver con la información, tratamiento y recolección de datos de los colombianos.

Antes de ello, quisiera dar unos breves antecedentes de por qué es necesaria la protección contra quienes traten los datos de los colombianos en internet señor Ministro, y hay unos antecedentes muy próximos, todos sabemos que los 2 grandes bloques digamos comerciales, o 2 de los grandes bloques comerciales, hablo de la Unión Europea y la Unión Americana, hay una distinción en el tratamiento de los datos, los europeos son mucho más firmes, más severos, más exigentes en cuanto a los niveles de protección de los datos de sus ciudadanos al paso que los Estados Unidos, sobre todo ahora que asumió una nueva administración, no tienen el mismo nivel adecuado de la protección de los datos.

Y en ese orden de ideas el tribunal europeo en un juicio de Chren contra Facebook ha dicho como concluido que los Estados Unidos no garantiza un nivel adecuado de protección de los datos personales de los ciudadanos europeos que son manejados por los Estados Unidos, en consecuencia, en ese mismo proceso judicial, se anuló el Acuerdo Safe Harbor por el cual las grandes empresas aseguraban proteger los datos que recababan y que los transferían a los Estados Unidos y los distribuían al cabo de un tiempo.

En cuanto a Facebook también hay que registrar que en Colombia siendo uno de los países de Latinoamérica con mayor penetración en las redes sociales, particularmente en Facebook, en Colombia hay aproximadamente 29 millones de usuarios de las redes sociales, esta red social registro solicitud de datos por parte de las autoridades de casi un 13 por ciento de sus usuarios.

Es decir, se recibieron solicitudes gubernamentales de datos privados de usuarios para hablar solamente del 2015, de casi 46.000 peticiones a nivel mundial, ¿qué quiere decir esto? Que los gobiernos están interactuando con las redes sociales solicitándole a esas empresas que faciliten los datos que tienen almacenados de los ciudadanos en muchas partes del mundo.

El Acuerdo Safe Harbor que regulaba la información y el tráfico de datos entre en la Unión Europea y los Estados Unidos decayó para darle paso a un nuevo esquema de cooperación a través del escudo de privacidad, que es el nuevo convenio rector de la información que entre en los Estados Unidos y la Unión Europea se intercambia y en Colombia aunque son pocos los datos, ya la Superintendencia de Industria y Comercio ha ordenado en algunos casos como a la Sociedad Geoestima S.A.S. el bloqueo temporal de la información de una usuaria que presento una queja ante la Superintendencia, porque no se le accedió en forma, tiempo y lugar el derecho acceder, corregir o actualizar información que de esta usuaria reposaba en esa base de datos.

También Uber, la plataforma de transporte, entrego datos de 14 millones de usuarios al gobierno de los Estados Unidos y colaboro en más de 400 solicitudes de investigación de robos de tarjetas de crédito, proporcionando como hemos dicho ya información sobre casi 14 millones de usuarios, conductores y pasajeros a diferentes agencias reguladoras de los Estados Unidos.

Sin duda, este tema señor Superintendente, yo quisiera que en este debate lo pudiéramos manejar con una información muy sencilla y al mismo tiempo relevante en términos muy llanos frente a lo que a nuestro juicio y también de otros actores como va a determinarse en este debate, queda claro la exposición que en adelante luego de la expedición de la circular expedida por su despacho, el pasado 5, la circular 5 del mes de agosto de este año, a nuestro juicio queda muy expuesta la información de los colombianos.

Y la frase pudiera ser una, la frase es que Colombia es el primer país señor Ministro, el primer país que, de manera oficial, es decir a nivel gubernamental, valida o da constancia o expide fe, que para todos los efectos es lo mismo, de que los Estados Unidos tiene un nivel adecuado de protección de los datos de sus ciudadanos en la legislación interna.

Esa que pudiera ser la idea central que desarrolla la Circular 05 expedida por la Superintendencia de Industria y Comercio, nos mueve a este debate y vamos a demostrar porque en las respuesta que da el Superintendente de Industria y Comercio se muestran muchas precariedades, muchas falencias y no poca ausencia de conceptos, que nos permite a nosotros solicitar como lo vamos a decir de una vez el retiro de esa circular, la revocatoria de esa circular por las razones que vamos a exponer seguidamente.

Miremos un poco el mapa, el primero de ellos para mirar a nivel mundial, allí esta señor Ministro y señor Superintendente el mapamundi donde los países que aparecen en azul son países que tienen algún tipo de regulación interna expedida bien por el Congreso o por el gobierno y que dan cuenta de que hay una norma que protege de alguna manera la información, el tráfico y el almacenamiento y recolección de la información de los ciudadanos en esos países.

Los que están señalados con rojo son países que no tienen ninguna norma, porque están pendientes precisamente de la expedición de normas que lo protejan y las que están en blanco y allí se incluyen los Estados Unidos de Norteamérica, no tienen una iniciativa o no existe una información de que de manera regulatoria o normativa se proteja los datos de los ciudadanos en esos países.

Entonces en el cuestionario que nosotros enviamos a la Superintendencia de Industria y Comercio, la primera pregunta señor Superintendente nos deja más preguntas que respuestas, que ofrece su despacho, porque la primera pregunta al cuestionario es ¿si existe o no tratado o convenio vigente y jurídicamente vinculante entre los Estados Unidos y Colombia para el tratamiento de datos personales? La respuesta no deja lugar a dudas, su despacho dice no hay un tratado o convenio específico suscrito entre los Estados Unidos de América y Colombia para el tratamiento de los datos personales.

Si no hay ningún tratado señor Superintendente y tampoco hay una legislación federal concreta sobre la protección de datos ¿Cómo se pretende garantizar la protección de los datos de los colombianos con una simple circular que le de alcance a una legislación que es ausente, que es etérea a nivel federal en los Estados Unidos máxime, como cuando lo vamos a demostrar aquí también, la nueva administración de Donald Trump, ha levantado prohibiciones de protección que había para los ciudadanos extranjeros en los Estados Unidos y por supuesto allí caen millones de colombianos que también viven en la nación del norte.

Otra pregunta del cuestionario se refería a la reciprocidad, ha si existía algún documento de las autoridades de los Estados Unidos que declararan formalmente a Colombia como un nivel, que tenía un nivel adecuado de protección de datos, la respuesta del Superintendente tampoco deja ningún atisbo de duda, dice: no hay ningún documento de las autoridades de los Estados Unidos que declare formalmente a Colombia como un país con un nivel adecuado de protección de datos, lo anterior teniendo en cuenta que su régimen legal no establece dicha figura y tampoco, agrega el Superintendente en su respuesta, hay documento alguno de las

autoridades de los Estados Unidos que permita que personas naturales o jurídicas ubicadas en territorio colombiano puedan recolectar o tratar datos de ciudadanos americanos.

Recordemos señor Ministro que en Colombia si existe una ley que precave todo lo relacionado con el tratamiento, recolección y circulación de datos que es la 1581 del 2012 independiente de la nacionalidad del titular de la información o del responsable del tratamiento.

Luego, la precariedad de esas respuestas, por muy sinceras que aparezcan, nos llevan a nosotros a pensar que hay señor Superintendente, se puede constituir una grave lesión para el buen nombre de los colombianos en empresas que trasladen lo sport en esta información a los Estados Unidos.

Otra pregunta: ¿Cómo se han manejado hasta ahora la recolección, almacenamiento, uso y circulación, y en general cualquier tipo de operación efectuada por empresas norteamericanas y que involucran datos de connacional, estamos viendo el espejo desde los Estados Unidos hacia Colombia? y la respuesta del Superintendente dice: la Superintendencia de Industria y Comercio no tiene información al respecto; ahí hay otro vacío que no deja lugar a dudas de que esta Circular 05 expone y de manera grave los datos de los colombianos.

A la pregunta número 6 del cuestionario ¿sírvase informar cuales personas naturales o jurídicas de los Estados Unidos actualmente tratan datos de colombianos, indicando el volumen de información que recolectan, almacenan, usan o circulan? Nuevamente el Superintendente de Industria y Comercio responde que no tiene información al respecto.

Entonces lo que nosotros deberíamos en este punto del debate señor Ministro y señor Superintendente y señora delegada, preguntarles a ustedes como máximas autoridades ¿acaso no es la 1581 del 2012 suficiente para la protección de los datos de los colombianos? ¿No tiene entonces competencia la Superintendencia de Industria y Comercio para proteger de manera adecuada los datos de los connacionales?

Hay en cambio como se deduce de las respuestas del Superintendente, un vacío legal para la protección de datos cuando se trata de transferencia internacional de los datos, como esta que permite la Circular 05 hacia los Estados Unidos.

¿Cuáles son entonces señor Superintendente y señora Delegada, cuales son las funciones y las competencias, las herramientas o instrumentos que tiene la Superintendencia para hacer valer los derechos de los colombianos cuando hay una sobre exposición, una vulneración de sus derechos al buen nombre por autoridades de otros países?

Y aquí viene algo que a nuestro juicio es bastante débil en la formulación de esa circular señor Superintendente, en la pregunta numero 7 nosotros le solicitamos a su despacho que se sirva remitir el estudio mediante el cual se estableció la factibilidad de permitir el tratamiento de datos de ciudadanos colombianos por empresas norteamericanas ubicadas en territorio de los Estados Unidos.

Esto como consecuencia del fallo de constitucionalidad de la Corte que prescribe que debe haber un estudio de factibilidad de parte del organismo en Colombia, esto es de la Superintendencia de Industria y Comercio para poder expedir una normativa de esta condición y calidad.

Y se anexa la copia de un estudio elaborado por le firma Valbuena Abogados S.A.S. el estudio es sobre la aplicación en Colombia de las normas sobre transferencia internacional de datos, pero cuando nos ponemos a ver de qué fecha es ese estudio, oh sorpresa, el estudio es del año 2013, es decir, es un estudio desactualizado, han pasado cuatro años, estamos en el 2017 y la Superintendencia de Industria y Comercio está dando un paso enorme, muy riesgoso para la adecuada protección de los datos de los colombianos, basando la circular señor Ministro en un estudio del año 2013.

Un estudio que entre otras cosas hablaba y habla ese estudio del Acuerdo Safe Harbor que había entre la Unión y los Estados Unidos cuando ese convenio de Safe Harbor de puerto seguro, ya fue derogado entre los Estados Unidos y la Unión Europea y ahora está en ciernes el escudo de privacidad.

Entonces estamos tomando una norma que ya no está vigente en la elaboración de ese estudio para tomar una decisión administrativa que es bastante riesgosa como hemos dicho para la tratativa de los datos de los colombianos.

Y miremos un poco que han dicho las 2 sentencias marco de la constitucionalidad que cita al estudio, hablo de la 748 del 2011 que se refiere a la 1581 y de la Sentencia C-1011 del 2008 que se refiere a la Ley 1266 lo más importante que dice entre otros asuntos esa sentencia es que en la posibilidad de entregar por parte de un operador colombiano a un empresa u operador extranjero tiene que haber una previa verificación de que las leyes del país respectivo donde se va a exportar la información, en este caso los Estados Unidos, hay la garantía suficientes ha dicho la Corte para proteger los derechos del titular de esa información.

Y ya hemos dicho que en Estados Unidos y es bueno recabar en esto señor Presidente, no hay una ley general de protección de datos como si la hay en Colombia con la 1581 o la 1266, lo que hay son acuerdos específicos, no leyes generales sino acuerdos específicos.

Y esa misma sentencia de la Corte Constitucional dice que la Superintendencia de Industria y Comercio y Financiera, quienes

deberán analizar el cumplimiento de los estándares de garantía de los derechos predicables del titular en el dato personal, en la legislación del banco de datos extranjero de destino.

Entonces dichas entidades, dice la Corte Constitucional podrán inclusive identificar expresamente los ordenamientos legales extranjeros, respecto de los cuales luego de un análisis suficiente pueda predicarse dicho grado de protección suficiente de los derechos del sujeto concernido.

Queda claro señor Superintendente que el estudio base para tomar la decisión de expedir la Circular 05 de la Superintendencia de Industria y Comercio es un estudio del año 2013 que está desueto frente a las exigencias nuevas del nivel de protección que se debe predicar de los sujetos cuya información o titularidad vayan a ser exportados a otros países.

Y hay algo muy importante aquí, que es lo que la Corte Constitucional y la misma 1581 han llamado el derecho de la parte de entregar el consentimiento previo, a ese operador para que su dato, previo consentimiento del titular pueda ser transferido por un operador a un banco de datos en el extranjero.

Estos requisitos de la Corte no pueden enviarse, quiere decir que la Ley 1581 y el mismo estudio de Valbuena lo prescriben, dice que tiene que haber de parte del operador el consentimiento previo y expreso del titular para que se pueda transferir el dato a un banco de datos nacional o extranjero.

De lo anterior entonces se colige, que el país al que se transfieran los datos no podrá proporcionar un nivel adecuado e inferior al contemplado en la legislación nacional, si una de las primeras decisiones que tomo la administración Trump, fue la de levantar la reserva sobre la información legal de ciudadanos no estadounidenses en territorio americano, queda claro que con esta decisión de la Superintendencia, queda totalmente expósita la información, de ciudadanos colombianos en el país del norte por cuenta de la validación que hace de la certificación de la constancia que expide Colombia, que es o bien hacer el único país, el primer país que en el mundo certifica a través de su gobierno que los Estados Unidos tienen un nivel adecuado de protección de los datos.

Quisiera además expresar señor Superintendente algo que es muy delicado, la respuesta que da a su despacho frente al cuestionario, se refieren al manejo de ciertos datos, por ejemplo, los datos comerciales, pero no se refieren al manejo integral de los datos privados, semi privados, sensibles y de los menores de edad.

Recordemos la prevalencia constitucional que tienen los derechos de los niños, en el artículo 44 de la Constitución, aquí evidentemente se trata de darle vía libre a todo tipo de datos para que puedan ser exportados de Colombia sin importar si esos datos son o no comerciales sino datos muy sensibles que atañen por ejemplo a la ideología, a la intimidad y mucho más cuando se trata señor Ministro de datos que sean de los menores de edad.

Yo he seguido de cerca la discusión y la participación suya doctor Luna en algunos foros en donde ha puesto de presente la necesidad de darle una regulación normativa al uso del internet en Colombia, sin restringirlo, porque es un derecho fundamental.

Por supuesto no solamente consagrado para todos los ciudadanos, sino que debe tener todos los días una mejor posibilidad de desarrollarse en el país, pero para nadie es un secreto que, en materia de redes sociales, eso se da un tráfico de información de todo tipo que muchas veces lesiona y de qué manera el buen nombre de quienes son sujetos pasivos en esas redes sociales y por eso en buena hora creo yo su despacho ha propuesto ciertos acuerdos de códigos de conductas que nosotros creemos que son necesarios para que sin restringir el uso de internet en Colombia y de las redes sociales, se le puedan poner responsabilidades a los usuarios también.

Y quiero también referirme a una respuesta totalmente imprecisa que da el señor Superintendente cuando se le pregunta en el cuestionario que otro país del mundo ha declarado los Estados Unidos como un país con nivel adecuado de protección de datos en los mismos términos que lo hizo la SIC en la Circular número 5 del 2017 y dice en la respuesta: la Unión Europea declaro a los Estados Unidos de América un país con nivel adecuado de protección respecto de empresas certificadas en el marco del escudo de privacidad.

Esa no es una respuesta, no es una respuesta precisa, porque ese acuerdo no declara a los Estados Unidos como país con un nivel adecuado de protección de datos, sino que dice que la Unión Europea podrá hacer transferencia de los datos de los europeos al suelo americano en aquellas empresas que prediquen un buen nivel adecuado de protección, empresas, no el territorio de los Estados Unidos de acuerdo al escudo de privacidad y que si cumplan las garantías que los europeos exigen.

Entonces quisiera también recabar en lo que dice la Universidad de Harvard que por supuesto es un centro académico referente de la mayor importancia y trascendencia, dice que en cuanto a la privacidad del internet, la Universidad de Harvard y esto es muy reciente, de menos de 1 mes, el 24 de agosto del 2017, dice que de hechos los usuarios de internet en los Estados Unidos tienen un nivel de protección inferior al de muchos otros países y que en abril de este año, dice la Universidad de Harvard el mes pasado, en abril de este año el Congreso Americano voto para permitir que los servicios de internet de los proveedores de

internet de Estados Unidos pudieran ser vendidos o transferidos a otros países.

Por el contrario, en la unión europea hemos conocido de multas a empresas como Google o como Facebook, muchas de ellas recientes como la que ocurrió en España el mes pasado cuando se multo a Facebook por inadecuado manejo en la protección y almacenamiento de los datos de los españoles con 1.2 millones de euros, esto nos debe llamar la atención sobre porque si Colombia viene dando señor Superintendente y señor Ministro unos pasos en la dirección indicada para elevar el nivel de protección de datos.

Y las dos leyes referentes la 1582 y la 1266 iban en la dirección indicada, ahora lanza prácticamente, da un paso como al vacío, con relación a esa misma protección de los colombianos expidiendo una circular, la 05, donde clasifica a los Estados Unidos, cosa que no ha hecho ningún otro país en el mundo como un país cuya legislación tiene un nivel adecuado de protección de datos.

Quiero terminar para reservarme algunas conclusiones y escuchar a los altos funcionarios invitados, quiero hacerle una invitación al doctor Luna, lo mismo que al Superintendente y a la Delegada de Protección de Datos, al igual que hicimos con la 1266 en un espacio de tiempo bastante largo, de casi 2 o 3 años, en donde en reuniones de trabajo, con todos los actores públicos y privados, pudimos consensuar la elaboración de lo que hoy se conoce como la primera ley de protección de datos en Colombia la 1266.

Ahora mismo estamos desarrollando una ley, un proyecto de ley que tengo que reconocerlo señor Ministro tuvo de parte de esta Comisión el apoyo unánime de los Senadores en ese momento presentes, 15, que votaron a favor del proyecto de ley nuestro también trabajado con actores, con representantes, de los distintos sectores de protección de datos en Colombia para sacar adelante una ley señor Ministro que de alguna manera le ponga unas reglas a las empresas que operan datos de los colombianos, en suelo colombiano, pero que no tienen un domicilio registrado en Colombia.

Y que obviamente cuando a cualquier usuario de esas empresas y hay ahí de todo como en botica, hay empresas muy importantes con un gran renombre a nivel mundial como Google, como Microsoft, como Twitter, Instagram, Facebook, que son empresas que por supuesto tienen códigos de regulación internos muy importantes, al mismo tiempo hay empresas que recolectan y almacenan sin ningún control los datos de los colombianos, sin que tenga ningún tipo de responsabilidad y cuando al ciudadano colombiano señor Ministro se le presenta un problema, tiene que irse como decía un profesor de derecho mío en la Universidad del Rosario, a quejarse al mono de la pila.

Porque la Superintendencia no tiene las facultades para exigir en nombre de ese colombiano que se le restituyan sus derechos al buen nombre.

Por eso ese proyecto de ley que ya iba cursando en la plenaria del Senado de la República, lo estamos trabajando, lo volvimos a presentar y yo quisiera invitarlo a usted señor Ministro, lo mismo que al Superintendente Robledo y a los funcionarios que están aquí a que sigamos trabajando ese proyecto, porque nosotros no somos enemigos, quiero ser claro en ello, nosotros no somos enemigos de que los colombianos hagan uso masivo y cada vez mejor y más activo de las redes sociales o del ciberespacio.

No, a lo que nos oponemos es a que, en ese tráfico de información, el buen nombre de los colombianos que resulta afectado por el uso de esas redes sociales son tenga ningún tipo de protección, para que, quejándose del usuario, quejándose el ciudadano se le pueda restituir o restablecer su buen nombre, inclusive acudiendo a sanciones de tipo administrativo o de tipo penal.

De suerte señor Ministro que yo lo quiero invitar a usted y al Superintendente a que trabajemos en ese proyecto de ley que ya hemos avanzado aquí en esta comisión y lo mejoremos, porque la idea es mejorar el proyecto de ley y permitirles a los colombianos que, desde el punto de vista institucional, llámense Congreso o gobierno están trabajando para elevarle el nivel de protección.

Con esas argumentaciones señor Presidente, yo quisiera dejar aquí para resérvame un espacio en las conclusiones luego de oír a los altos funcionarios citados y agradeciéndole a usted el tiempo que me ha dispensado señor Presidente, muchas gracias.

La Presidencia ofrece el uso de la palabra al doctor Pablo Felipe Robledo del Castillo – Superintendente de Industria y Comercio:

Bueno, muchas gracias señor Presidente por este debate y al Senador Amín también un agradecimiento por este debate, a los demás miembros de la Comisión que nos acompañan.

Sé que en la sesión pasada Senador Amín hubo algún nivel de inconformidad por la ausencia particular del Superintendente, yo simplemente quiero referirme a ese tema diciéndole había una primera citación, tal vez para el 5 de septiembre, un día martes, yo cambie mi agenda, porque a mí me gusta venir a los debates y dar las explicaciones de rigor.

El lunes de la semana pasada habíamos tomado una decisión muy importante que el país la ha visto en relación con el tema del futbol colombiano y tuve una reunión absolutamente urgente e inaplazable sobre ese tema y por eso no vine.

Pero quiero decirle que hoy y se los digo porque también hay un debate de control político en las horas de la tarde en la plenaria, al que no voy ir porque estoy enfermo, tengo amigdalitis, aquí

está mi excusa médica de 3 días, pero obviamente vine a este debate aun teniendo una incapacidad médica, pero 2 debates de control político si no aguanto con amigdalitis el mismo día.

En relación con este debate, yo festejo y lo hago incluso tomándome la vocería del Ministro encargado de Comercio y del Ministro de Comunicaciones, agradecerle a usted el debate y el tono en que se ha hecho el debate y la forma como se ha presentado el debate, porque me parece que de estos debates lo importante es que salgan cosas constructivas y reflexiones constructivas para todos los que somos actores en la protección de datos personales, que empieza desde el propio Congreso que hace las leyes y las entidades públicas que tenemos la obligación de proteger los datos personales de los colombianos.

Luego le agradezco particularmente el debate, siempre lo digo, en lo que hace la Superintendencia de Industria y Comercio es importantísimo venir al Congreso a dar las explicaciones que haya que dar, a quien haya que darlas, en lo que hacemos para proteger la libre competencia económica, proteger a los consumidores y proteger al hábeas data.

Aquí particularmente vinimos hace un parte de años a esta comisión a un debate que hizo Luis Fernando Velasco, también que tenía inquietudes sobre un decreto que había sacado el gobierno nacional muy inspirado como todos estos temas del hábeas data en decisiones de la Superintendencia de Industria y Comercio, el en su momento le auguraba un mal futuro en el Consejo de Estado.

Él decía que ese decreto era inconstitucional, era ilegal, que desbordaba la ley general del hábeas data y la verdad es que ese decreto aun años después sigue vigente, pero el debate obviamente tenía fundamento y lo llevamos en muy buenos términos como corresponde.

Yo comparto lo que usted ha dicho en relación con la gran evolución y esto lo hago en el ánimo absolutamente constructivo y realista de la protección de los datos personales de los colombianos, que hemos tenido en Colombia, en Colombia ni siquiera hasta fruto de la 1266 y no fruto de la ley estatutaria, logramos desde el punto de la institucionalidad lograr sacar la protección de los datos personales de los jueces de tutela.

Durante mucho tiempo no hubo ninguna protección de los datos personales de los colombianos, con la Constitución del 91 y por 2 décadas, la protección fue absolutamente aislada, cliente por cliente, es decir Pedro, Juan o María, el problema de cada uno de ellos, pero no hubo una política pública de protección de los datos personales.

La Superintendencia fue reformada, creamos una delegatura, fruto de los mandatos legales, para proteger los datos personales igual que protegemos los consumidores o de libre competencia económica, etc., entonces hay toda una infraestructura administrativa que yo realmente la considero valiosa por el pasado, pero la considero insuficiente por el presente y por el futuro.

Yo quisiera obviamente que esa delegatura tuviese más presupuesto, que tuviese más gente, pero diríamos ahí hay una evolución institucional, evolución institucional que nos ha permitido como autoridad de protección de los datos personales de los colombianos tomar acciones, no solo discursos, sino tomar acciones, hemos investigado un sinnúmero de empresas en Colombia que han violado los datos personales de los colombianos, los hemos sancionado, hemos impuesto sanciones importantes y al mismo tiempo le hemos solucionado el problema a miles y a miles de colombianos, por lo que se considera una infracción a sus datos personales.

Pero aquí quiero hacer una reflexión sobre la legislación vigente, usted ponderaba la legislación vigente y lo ponderaba haciendo un reconocimiento de su propio protagonismo en el desarrollo de esas leyes que me parece que es real y que es valioso y que lo pone a usted como un interlocutor absolutamente valido para hablar de este tema y propender porque haya una mejor protección de los datos personales de los colombianos.

Pero claro que tenemos que emprender como en muchas cosas unas modificaciones al régimen legal, no es posible que una empresa que de manera sistemática generalizada y grave viole los datos personales de los colombianos y que la máxima multa que la autoridad de protección de los datos personales pueda imponerle sea de 2.000 salarios mínimos, es decir, 1.500 millones de pesos, 1.500 millones de pesos muchas de esas empresas terminan incluso riéndose del estado cuando los investiga y los sanciona.

Yo eso no solo lo he dicho para hábeas data, también lo he dicho para temas de competencia, como es posible que una empresa que se cartelista en Colombia no tenga una multa sino de 75.000 millones de pesos, cuando en todos los países del mundo, civilizados, desarrollados, la capacidad sancionatoria va muchísimo más allá, porque es la forma adecuada de sancionar carteles empresariales.

Entonces claro que a las leyes que hoy rigen la actividad de la Superintendencia de Inspección, vigilancia y control hay que hacerle una modificación y la ley de hábeas de data no se escapa a ese tema.

Hay una verdad de apuño, y usted lo referenciaba, la ley general de protección de datos personales en Colombia tiene una marcada inspiración europea, en el mundo diríamos, que valga la pena mencionar hay 2 tendencias legislativas, y hasta de concepción de la protección de los derechos de hábeas data, una es la europea y la otra es la de Estados Unidos, la mal llamada americana.

Colombia como muchos temas, este no es el único, se han inspirado en la filosofía y la forma de concepción legislativa de Europa y la ley general como usted lo decía, la Ley 1581, pues es fruto, está inspirada diríamos en las normas europeas, principalmente en la Directiva Europea 9546.

El tema que a nosotros nos convoca a este debate de control político es una disposición que hizo el Congreso, no es de la Superintendencia, la hizo el Congreso en la ley estatutaria, que regula el tema de la transferencia de datos, es decir, unos datos recogidos en Colombia que se envían a otras partes del mundo para que sean almacenados o para que sean tratados en otras partes del mundo de acuerdo con las instrucciones que para tal efecto le hagan la compañía que recogió los datos en Colombia, que es lo que genéricamente se conoce como la transferencia de datos.

Esa ley estatutaria en el artículo 26 ordeno algo que yo creo que es bien concebido y es importante que esos datos de los colombianos recogidos en Colombia no pueden ser enviados, no pueden ser transferidos a compañías en otros países del mundo, si esos otros países del mundo no tienen un adecuado régimen de protección, es una palabra creo yo bastante importante, adecuado régimen de protección.

Y que es la Superintendencia de Industria y Comercio, no el Ministerio de las TICS, no el Ministerio de Comercio, eso lo dice la ley, es la Superintendencia de Industria y Comercio quien tiene que establecer los parámetros para poder catalogar a un país con régimen adecuado de protección o eventualmente tomar la decisión de que un país tiene un régimen inadecuado de protección.

Y previamente como usted muy bien lo menciono, eso obviamente esa información que se recoge en Colombia tiene ciertas excepciones, es decir, uno podría transferirlas a un país que no cumpla el estándar siempre y cuando estén unas excepciones consagradas en el propio artículo 26, pero diríamos eso no es lo que me incumbe en este momento.

Para determinar los estándares adecuados de protección, ustedes saben que hay una ley estatutaria, esa ley estatutaria antes de ser ley, pues entonces va a la Corte Constitucional para el control previo de constitucionalidad y la Corte en la sentencia que usted cito, en la Sentencia 748 del 2011 pues se pronunció, y se pronunció como se pronuncia artículo por artículo y cuando llego al artículo 26 pues digo lo que digo.

¿Y qué digo la Corte? También hace mucho tiempo, en el año 2011 digo pues lo que tenía que decir, que la Superintendencia de Industria y Comercio es la autoridad por delegación si se quiere del Congreso de establecer los parámetros para catalogar a un país con adecuado régimen de protección de los datos personales.

Segundo, que en ese estudio o en la valoración de si un país tiene un régimen adecuado de protección de hábeas data, de datos personales, debe pretenderse que en ese país no haya un estándar inferior al colombiano, o sea que lo que uno tiene que encontrar en ese país, ojalá encontrara más, pero como mínimo tiene que encontrar lo de Colombia y dio unas pinceladas sobre lo que uno debería encontrar y fundamentalmente la lectura que le hace la Superintendencia a lo que la Corte digo en el control previo de constitucionalidad es mire si ese país tiene una normatividad que proteja el hábeas data, que tenga ciertas características, mire la institucionalidad que ese país tenga para proteger el hábeas data y en la institucionalidad pues mire las autoridades administrativas y mire las autoridades judiciales.

Y si después de hacer esa valoración la Superintendencia llega a la conclusión que ese país tiene un régimen adecuado de protección, pues tiene un régimen adecuado de protección, si después de analizar eso llega a la conclusión de que no, pues no tiene un régimen adecuado de protección.

Entonces la Superintendencia se dio a la tarea de cumplir ese mandato de la ley estatutaria de establecer los criterios para determinar que un país tiene un régimen adecuado de protección que viabilice las transferencias.

Ese trabajo Senador Amín, Senadores podía hacerse de dos maneras, o sea, en el proceso de lo que termino siendo el Circular 005 elaborada por la Súper, ese mandato de establecer los parámetros podía hacerse de dos maneras.

1. Enlistando simplemente los parámetros que uno evaluaría como autoridad de protección de datos personales en Colombia respecto de otro país, entonces si cumple a), b), c), d) y f) pues ese país eventualmente frente a una investigación uno termina diciendo que cumplió y si no pues que no cumplió.
2. Lo otro era haciendo una lista de países previamente evaluados que a la Superintendencia le diera la tranquilidad de ser un país con un adecuado régimen de protección.
3. Y como siempre que hay dos posibilidades surge una tercera, que era hacer una mezcla de ambas formas de hacer la circular.

¿Entonces qué terminamos haciendo? Terminamos estableciendo unos parámetros, pero haciendo un inventario de países que a la Superintendencia como autoridad de protección de datos le dan tranquilidad en relación con el hecho de que son países que tienen un régimen adecuado de protección.

Los que están en la lista, diríamos para poder explicarlo sencillamente, están certificados como país, por llamarlo de alguna manera, el país que no aparezca en la lista no quiere decir que este desertificado, sino que frente a una investigación

habría que acreditar que los datos personales fueron enviados a determinado país y que ese país cumple el requisito a), b), c) y d).

Para hacer la lista la verdad miramos el estudio de hace unos años, tal vez del año 2013 que elaboro un ex Superintendente de Industria y Comercio el doctor Valbuena, Gustavo Valbuena ex Superintendente del anterior gobierno, de finales del gobierno del Presidente Uribe, que fue contratado por la Superintendencia de Industria y Comercio.

Y el hizo un examen de una cantidad importante de países y a criterio de él, no de la Superintendencia, porque él fue el que hizo el estudio, pero expreso su criterio, el listo unos países y dijo estos países cumplen y estos países eventualmente no cumplen y considero el que tenía un régimen inadecuado de protección o por lo menos no suficiente.

Con base en ese estudio y otras fuentes de información y otros documentos que nosotros analizamos en el momento, expusimos al país para cometarios de terceros, como frente a todo proceso regulatorio hay que hacerlo, el borrador de circular y nosotros no incluimos a los Estados Unidos, incluimos a una cantidad importante de países, pero no incluimos a los Estados Unidos y no incluimos a los Estados Unidos porque inicialmente al hacer la evaluación de los Estados Unidos consideramos que los Estados Unidos si bien tiene un régimen de protección y unas normas de protección de los datos personales no estaba en consonancia con los criterios de la Corte Constitucional y lo que había dicho la ley estatutaria frente a declararlo como un país adecuado, con nivel adecuado de protección.

Nosotros publicamos para comentarios ese decreto y una cantidad importantísima de gremios, entidades, académicos, empresas, nacionales, internacionales, no sé, 40, 50, 60 comentarios, una cantidad importante hicieron glosas a la circular y casi todas esas glosas estuvieron encaminadas al tema de Estados Unidos.

O sea, no se el porcentaje, pero podría aventurarlo, el 85 por ciento de las glosas o el 80 por ciento de las glosas estaban encaminadas a si Estados Unidos debía estar o no incluido en esa lista.

Mayoritariamente la gente digo se les quedo Estados Unidos por fuera, no vayan a cometer el error de dejar a Estados Unidos por fuera, algunas personas pues dijeron lo contrario, muy bien que no hayan incluido a Estados Unidos.

Eso lo cuento sencillamente para decirles sencillamente a partir de ese momento en el gobierno existió la preocupación, bueno, ¿y qué vamos hacer con Estados Unidos? Y el gobierno empezó a trabajar de manera conjunta y trabajamos con la CRC, que está aquí presente, ahí está el comisionado Germán Enrique Vaca Medina y el doctor Wilches, trabajamos con la CRC, trabajamos con el Ministerio de las Tecnologías de la Información y la Comunicación TICS y trabajamos con el Ministerio de Comercio.

Y tuvimos muchas reuniones, muchas reuniones con los empresarios, nacionales y extranjeros, con la embajada de los Estados Unidos, con embajadas incluso de otros países que nos decían oiga ¿y por qué este determinado país no fue incluido? E hicimos unas mesas de trabajo.

Al final Senador Amín, la Superintendencia para no hacer muy larga esta historia, la Superintendencia se convenció, quedamos convencidos de que había sido un error de la Superintendencia el haber excluido a Estados Unidos de ese primer borrador y por eso en la versión final se incluyó además de muchos otros países, pues o sea, la lista, incluimos a Estados Unidos, en la lista esta Alemania, Austria, Bélgica, Bulgaria, Chipre, Costa Rica, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Estados Unidos de América que fue incluida, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Lucemburgo, 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.

Entonces mire la lista, mire la categoría de países, y yo francamente puedo entrar en el debate y en las explicaciones en relación sobre si un determinado país de esta lista debiera estar en la lista o no, lo que yo le quiero decir es que el problema no se circunscribe únicamente a Estados Unidos y aquí hay otros países, de mucha menor entidad que los Estados Unidos y sobre todos puede haber duda.

La Superintendencia equivocada o no considero que estos son los países que de entrada tienen un nivel adecuada de protección, sin que los que no estén ahí no puedan acreditar frente a una investigación que tienen un nivel adecuado de protección, entonces el tema no es solo Estados Unidos, es a lo que yo quería referirme.

Ahora ¿Por qué Estados Unidos? Si el debate es Estados Unidos y no es Letonia, pues ¿Por qué Estados Unidos? Pues por varias razones y yo obviamente, usted hablaba ahoritica del doctor Remolina, que yo lo reconozco como una gran autoridad en América Latina como usted lo dice sobre este tema, pero no es el único y entre autoridades académicas pues hay todo tipo de tesis, porque pues cuantos académicos no están de acuerdo con la inclusión de Estados Unidos, que los hay que no están de acuerdo con la inclusión de Estados Unidos pues también los hay.

Y los podríamos traer al debate, para que nos digan por qué razones están de acuerdo con la inclusión de Estados Unidos, lo que yo le quiero decir es que aquí no hay nada de perversidad, aquí

no hay nada de mala intención y aquí hay un tema de criterio.

Para usted seguramente es un error que se incluya Estados Unidos, para la Superintendencia es un gran acierto haber rectificado y haber incluido a Estados Unidos en esta lista que como le digo, en la que están incluidos muchos países.

¿Por qué Estados Unidos? Nosotros lo que empezamos por reconocer, perdóneme el paisa, en la patraciada, nosotros habíamos excluido a Estados Unidos y lo incluimos, entonces ahí la propia Súper se hecho de para atrás, ¿Por qué nos echamos de para atrás? Porque reconocimos que lo que la Corte Constitucional había dicho había que leerlo de manera más amplia y menos restrictiva como lo digo la Corte, porque finalmente lo que la Corte dijo, lo dijo en relación con sistemas jurídicos absolutamente afines a nosotros.

Y lo primero que entramos por reconocer es que Estados Unidos no tiene un sistema jurídico afín al nuestro, que ahí hay diferencias y formas distintas de proteger, lo que aquí se protege de una manera, allá se protege de otra manera, que son sistemas diferentes y buscamos una explicación tecnológica, finalistica.

¿Qué fue finalmente lo que dijo la Corte? Leyendo lo que la Corte dice pues uno advierte independiente de la manera como lo digo ¿Qué trato de decir? Oiga, no vamos a permitir como autoridad colombiana, como país, que se haga transferencia de datos que no presente garantías para la protección de los datos personales de los colombianos, eso no se puede permitir.

Entonces mirando Estados Unidos y entendiendo las diferencias ¿pues qué encuentra uno? Como usted muy bien lo dice, allá no hay una ley general de protección de datos personales, no la hay, ¿que yo quisiera que la hubiera? Pues claro que quisiera que la hubiera ¿Qué en Europa sí la hay? Sí, ¿Qué en algunos países de América Latina la hay? Entre otras cosas muy pocas y muy pocas tienen institucionalidad, eso se reduce a 4 o 5 países de América latina como muchas cosas de la tristeza de América Latina y África que es falta de institucionalidad.

Colombia es un país que la tiene, allá me viene generando datos personales, aquí en Colombia sí, pero miremos ¿qué hay allá? Porque no es que allá no haya nada, como usted también lo reconoce, entonces allá tenemos la ley de la Federal Trade Commission, la ley de política de comunicaciones por cable, la ley de protección de privacidad en línea de niños, la ley de protección de la privacidad de los conductores, ley de privacidad de comunicaciones electrónicas, ley de transferencia electrónica de fondos, Ley Grange Bridge Baile, ley del derecho de privacidad financiera, ley de protección del consumidor del teléfono, ley de protección de la privacidad de video, ley de reporte justo de crédito, ley de portabilidad y responsabilidad de seguro de salud y reglas de privacidad, ley de transacciones de crédito justas y exactas, etc., etc., etc.

Y todas estas leyes establecen niveles de protección de los datos personales, desde el punto de vista sectorial, miren que así empezó Colombia, la primera ley de protección de datos personales que tuvimos fue sectorial, que fue a la que usted se refirió, la Ley 1266 y después cogimos una ley general, Estados Unidos, pues le ha jugado a otra cosa, a hacer protecciones sectoriales en muchos sectores.

Entonces si bien en Estados Unidos no hay una ley general, hay una cantidad importante de leyes sectoriales, ¿Que conducen a qué? Pues no a que haya un régimen general porque no lo hay como lo digo la Corte, sé que la Corte digo ley general, pero la Corte teratológicamente lo que digo es que no hay desprotección, que haya un nivel de protección importante.

Entonces aquí hay unas normas, ¿Qué tienen los Estados Unidos'? institucionalidad, ojo, institucionalidad importante, nosotros casi no tenemos, casi no tenemos, nosotros llevamos dando los primeros pasos para proteger los datos personales de los colombianos, eso se queda reducido a los últimos 2, 3, 4, 5, 6 años.

En Estados Unidos lo que hay es institucionalidad, perdóneme y ese país es lo que es por la institucionalidad, eso no hay que saber mucho de geopolítica para entender que los países que tienen una institucionalidad importante son los países del primer mundo, los países desarrollados y en los que hay ausencia de institucionalidad, pues el subdesarrollo brota, que es uno de los casos de Colombia.

¿Qué hay allá en institucionalidad? Pues nada más ni nada menos que la Federal Trade Commission de los Estados Unidos, la Comisión Federal de Comercio, la Comisión Federal de Comercio protege la libre competencia, protege los consumidores y protege el hábeas data, igual que la Superintendencia de Industria y Comercio, pero con una diferencia, que ahí hay 300 millones de dólares, es decir, 1 billón de pesos de presupuesto para hacer la tarea y aquí en Colombia en el año 2010 no habían sino 38.000 millones de pesos para hacer la tarea, allá hay 1 billón.

Pero esa es una de las tantas entidades, la Comisión Federal de Comunicaciones, el departamento de salud y servicios humanos, la Oficina de Protección Financiera del Consumidor, la comisión de bolsa y valores, la Oficina de Protección Financiera del Consumidor, los procuradores generales del estado y las autoridades estatales.

Y como si fuera poco, como si fuera poco, tienen un sistema judicial, un sistema judicial, que hoy estamos en grave crisis en el sector de la justicia, la cual es una verdad de apuño, pues nosotros quisiéramos tener la venteaba parte de ese sistema judicial.

Tienen un sistema judicial que protege la gente, mucho mejor que el colombiano, entonces ¿A dónde voy? Voy a que cuando examinamos Estados Unidos y le digo Senador Amín, nos pudimos haber equivocado, o pudimos haber acertado, porque ese es un tema creo yo que tiene cierto nivel de subjetividad desde el propio criterio, que se llama la Superintendencia determinara si un país tiene un adecuado sistema de protección, un adecuado nivel de protección, tiene una dosis de subjetividad, para alguien será adecuado y para alguien no.

Entonces nos pudimos haber equivocado, pero no lo hicimos de manera inconsulta, ni lo hicimos de manera arbitraria, estudiamos las leyes sectoriales, estudiamos la institucionalidad y estudiamos el sistema judicial americano.

Y por esas razones la Superintendencia tomo la decisión de incluir a Estados Unidos en una lista, que eso no lo he dicho, que es en la que está incluida todos estos debates, todos estos países y la lista no está grabada en piedra, la lista está en una circular y el día que la Superintendencia de Industria y Comercio, advierta razones que lleven al convencimiento de la Superintendencia de Industria y Comercio, que un país no tiene adecuado nivel de protección.

Pues la Superintendencia, el Superintendente que este, yo o el que me reemplace, tendrá que tomar la decisión de modificar la lista de la circular, porque la propia circular pues lo dice: 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.

Entonces la lista no está grabada sobre piedra, la lista puede mutar, la lista puede cambiar el día de mañana, uno puede sacar a Estados Unidos, puede meter a Brasil, puede meter a Chile, puede sacar a Letonia, es decir, la lista no es inmodificable.

Y simplemente termino, por lo menos si quiere esta primera parte, comoquiera, para decir que la base de la legislación colombiana, para el tema de transferencia también está basada en un principio del cual hasta donde yo advierto usted no habló, pero me parece que es importante, no estoy diciendo con ello nada diferente a que creo que usted no lo digo.

Un principio de la responsabilidad demostrada, entonces, cuando una empresa recolecta datos en el territorio colombiano y los va a transferir, sigue respondiendo por la transferencia que hizo de los datos personales, no se desliga de la responsabilidad por la recolección y el tratamiento que el hizo de los datos personales y no puede desmontarse del caballo bajo la tesis de que hizo una transferencia internacional de datos; eso queda completamente claro.

Entonces cuando esos datos se recogen en Colombia, se tratan en Colombia y después viene la transferencia internacional de datos, a estos países de la lista, incluyendo Estados Unidos o a otro país que no está en la lista, pero que a criterio de quien los transfirió cumple con los estándares, los requisitos de nivel adecuado, no se desliga de su responsabilidad y la Superintendencia tendrá que investigar si ocurre alguna irregularidad en relación con quien hizo la transferencia de datos.

Ahora, yo también creo que nosotros tenemos que sentarnos a revisar un tema del que usted hablo demasiado y con gran propiedad, que es lo que guarda relación con la aplicación de la ley de hábeas data en el espacio, si nosotros tenemos o no la posibilidad como autoridad administrativa de investigar a una compañía que está ubicada en el extranjero, que no tiene participación en el mercado colombiano, que está recogiendo y tratando datos en el extranjero, datos de colombianos.

Porque ahí tenemos 2 problemas, uno es si la actual legislación lo permite y otro es que ya es un tema practico, que investigado y sancionado como hacemos nosotros para hacer efectiva la multa.

Es decir, una especie del exequatur si se tratara de una sentencia judicial ¿Cómo hacemos para que procesado en Colombia esa empresa extranjera que no tiene operación en Colombia, es sancionada, como hacemos que no se burle de la sanción que nosotros le pusimos y que podamos efectivamente cobrar las sanciones? Poquitas en cantidad de dinero o muchas si el día de mañana se modifica la ley.

Yo con eso termino y le repito, se lo digo de todo corazón, le agradezco el debate, me parece que es muy importante y es muy importante para Colombia y para los colombianos que nosotros que tenemos estas responsabilidades hablemos ante el país de un tema tan importante y tan sensible como los datos personales de los colombianos.

La Secretaria informa que se ha constituido quórum decisorio.

La Presidencia cierra la discusión del orden de día y sometido a votación es aprobado por unanimidad.

Atendiendo instrucciones de la Presidencia la Secretaría da lectura al siguiente punto del Orden del Día

II

Consideración y aprobación de actas

La Presidencia cierra la discusión de las actas: **Acta número 06 del 15 de agosto de 2017, publicada en la *Gaceta del Congreso* número 756 de 2017; Acta número 07 del 16 de agosto de 2017, publicada en la *Gaceta del Congreso* número 757 de 2017, Acta número 08 del 22 de agosto de 2017 publicada en la *Gaceta del Congreso* número 776 de 2017; Acta número 09 del 23 de agosto de 2017 publicada en la *Gaceta***

***del Congreso* número 768 de 2017** y sometidas a votación son aprobadas por unanimidad.

La Presidencia manifiesta que continúa el debate y ofrece el uso de la palabra al doctor David Luna Sánchez – Ministro de Tecnologías de la Información y las Comunicaciones:

Presidente muchas gracias, un saludo muy especial a todas las señoras Senadoras y a los Senadores, agradecerle muy especialmente la invitación al señor citante y efectivamente como lo hizo el señor Superintendente reconocer la importancia de este tema.

En un país donde tenemos tantas dificultades, pero también tantos temas, los de tecnología tienden a tener un espacio no tan grande como quisiéramos en realidad y hoy el doctor Amín ha planteado algunas reflexiones que me parecen tienen mucho de fondo, no solamente referente a la protección de datos, sino sobre otro tema que si usted me permite yo también quisiera comentar cómo es el del derecho al olvido.

Pero voy arrancar por el principio, yo tuve la fortuna de estar en esta corporación, no en el Senado sino en la Cámara en el año 2006 y fui coautor y ponente de una ley que usted también recuerda muy bien, porque fue como su hija, la 1266 del año 2008, en esa ley después de 17 intentos, en virtud de que es una ley estatutaria, el Congreso de la República después de muchos debates, logró sacar adelante tal vez el primer ejercicio de hábeas data que la Constitución había señalado en su momento.

Y vale la pena recordar esa historia por nada distinto que por entender dónde estábamos antes y dónde estamos hoy, anteriormente este era un tema que la literatura era muy constantemente discutido, pero que la aplicación era muy poco desarrollada, a tal punto que de alguna u otra manera no se trataba o no se exigían ningún tipo de reglas.

Yo veo que Colombia en ese entonces comienza una discusión muy interesante y recordará usted doctor Jaime, pero también muchos otros Senadores que estuvieron presentes, que entonces se hablaba de quién iba a ser la autoridad de protección de datos, entre otras razones porque ya lo dijo el doctor Pablo Felipe Robledo, nuestra ley tiene una influencia española muy grande.

Y España tiene una agencia de protección de datos totalmente independiente, Colombia no la tenía y adicionalmente no existía el presupuesto para crearla, motivo por el cual días o meses después, se toma la determinación que esa función quede en cabeza de la Superintendencia de Industria y Comercio con algo que pasa desapercibido.

Y fue que la recomendaciones Europeas decían bueno, avancen en ese sentido, pero con una especial condición, que ese Superintendente sea de libre designación y nombramiento, mas no de libre remoción, años después afortunadamente se tomó esa determinación en un decreto y no solamente el señor Superintendente, sino algunos otros como el financiero, y como el de sociedades tienen esa misma condición.

¿Por qué? Para garantizar la independencia en la toma de sus determinaciones y adicionalmente para permitir algo tan importante y tan valioso como es proteger al consumidor, esa ley del año 2008 tiene un desarrollo posterior que tiene mucho que ver con este sector, el de la tecnología, el año 2009, que lideró mi antecesora hoy Senadora de la República la doctora María del Rosario Guerra.

Que fue la transformación del sector de telecomunicaciones al sector de tecnologías de la información y las comunicaciones, y esa ley tiene grandes aciertos, pero para mí el más importante de los aciertos es haber incluido el principio de neutralidad de red.

Ese que no es un principio tecnológico desde mi punto de vista, sino un principio democrático es el que permite hoy que cualquier tipo de plataforma, cualquier tipo de plataforma ruede por la red de internet, salvo las que el Congreso expresamente prohíba y el Congreso se ha anunciado en esa materia en 2 oportunidades.

Una, la que hace referencia al contenido de pornografía asociado a los menores y dos la que hace referencia a los juegos en línea, lo demás ha dicho el Congreso debe ser respetado dentro del principio de la neutralidad de red y yo creo que el Congreso tanto en el año 2008 como en el año 2009, como adicionalmente en estas últimas decisiones y determinaciones ha acertado.

Porque si usted analiza, cuáles han sido las determinaciones europeas o americanas tienden a ser mucho más progresistas las decisiones de este Congreso que incluso muchas otras, esto es muy importante y muy interesante ¿Por qué? Porque evidentemente como ya lo mencionó el señor Superintendente cuando inicia esta discusión, la misma nace de una ley expedida por el Congreso.

Pero en virtud de su condición de estatutaria, de una sentencia de la Corte Constitucional, que como siempre nos tiene acostumbrados a una valoración muy juiciosa y en ese momento de manera casi que puntual, artículo por artículo la Corte señala con que está de acuerdo, con que no y agrega adicionalmente una serie de obligaciones y de contenidos en este caso puntual y particular referente a ese tema de los países que garantizan o no la seguridad en la protección de los datos.

Y la Corte le entrega a la Superintendencia una serie digamos de garantías que le permiten esa valoración y que le permiten además esa discusión creo yo bastante importante y es por eso que la Superintendencia como lo hacemos todos en el Estado, entre otros por obligaciones relacionadas con normatividad internacional, publica para comentarios una circular que el sector público y

el sector privado reacciona ante ella con una gran cantidad de reflexiones.

Ya lo dijo el doctor Robledo, pero simplemente quiero repetirlo yo, sobre este tema en particular, si bien es cierto y en eso Senador Amín coincidimos con usted plenamente, Estados Unidos no tiene una reglamentación específica, si tiene una reglamentación que le permite entender que la protección de datos hace parte de la esencia del Estado en diferentes temas.

Pero segundo, algo mucho más valioso que lo primero y por eso es lo importante del debate además de muchas otras razones, la Superintendencia en virtud de su condición, de órgano administrativo, pero también en su condición de ente regulador de la protección de datos no solamente contempla, sino adicionalmente garantiza que este tipo de normas puedan ser no solamente revisadas, sino adicionalmente adicionadas.

Y yo creo que ahí hay un punto muy valioso del por qué estamos sentados hoy, usted nos está haciendo una serie de reflexiones, todas ellas a lugar, que tienen mucho que ver con decisiones que evidentemente pueden tener posiciones encontradas, pero esas reflexiones lo que permiten es demostrar que acá hay algo bastante importante e interesante, cual es el del principio de la responsabilidad demostrada.

Ya lo mencionó Pablo Felipe, lo repito, la empresa que maneja datos de orden colombiano, por llamarlo de alguna manera, jamás pierde esa responsabilidad si la nube por así decirlo está establecida en Estados Unidos, más del 85 por ciento de los datos, que están en la nube privada, pública o inclusive en la nube hibrida están alojados en los Estados Unidos y por eso es tan importante y tan interesante este ejercicio que estamos llevando a cabo el día de hoy.

Porque evidentemente fuimos varios órganos del Estado, el Ministerio de Comercio, la Comisión de Regulación de Comunicaciones, nosotros como Ministerio de Tecnologías, quienes acompañamos en la discusión a la SIC, pero la SIC tenía esa única responsabilidad como ente rector en materia de protección de datos a la toma de la determinación.

Yo creo y es un poco lo que entiendo como invitación suya cuando nos dice hay un proyecto de ley sobre el particular, nos parece interesante que esas mesas de discusión se puedan dar, que evidentemente pueda haber argumentos de diferente índole sobre esta discusión, que pueden ser discutidos.

Creemos que el gobierno actuó no solamente responsablemente sino adicionalmente oportunamente.

Creemos que la industria se siente no solamente oída, sino adicionalmente representada en esa determinación ¿Cómo se siente el consumidor? Que es lo más importante de todo, porque en esto de la digitalización el centro tiene que ser el usuario, tiene que ser el consumidor, tiene que ser el ciudadano que claramente tiene la responsabilidad de tomar determinaciones y decisiones en materia de sus datos.

Y es ahí donde yo me permito introducir otra herramienta adicional dentro del debate, el consumidor, lo sabemos nosotros tiene la potestad no solamente, porque así lo consagró la ley, sino así lo ratificó la sentencia de la Corte Constitucional, de estar de acuerdo o no estar de acuerdo con la utilización de sus datos, en determinadas bases de datos.

De hecho, casi todos, pero si no la gran mayoría de quienes están en este recinto envían informes de gestión y en esos informes de gestión tienden siempre a poner en la parte inferior o en la parte superior que los destinatarios de esos correos electrónicos están recibiendo esos correos electrónicos en virtud de la ley de protección de datos.

Y que, si no están de acuerdo con recibirlos, pueden hacer una de dos cosas, o solicitar su exclusión de esa base de datos o en su defecto solicitarle a quien está enviando ese correo no volver hacerlo.

Esa normatividad que de alguna u otra manera tiene una gran diferencia a lo que vivíamos en el 2008 a lo que estamos viviendo hoy en el 2017, lo que trata de transmitir es que el consumidor está en el centro de la operación.

¿Por qué este ejemplo? Porque la Superintendencia si bien es cierto emite la circular, incluye a los países que ya mencionó el doctor Pablo Felipe Robledo, no significa que no mantenga no solamente su ejercicio de control, sino adicionalmente de jurisdicción y en ese sentido nos parece a nosotros que es una garantía suficiente, en el entendido que un ciudadano consumidor, cliente, levante la mano hacia la Superintendencia y determine que sus datos no están siendo manejados de manera correcta, para que la Superintendencia no solamente pueda actuar en ese caso particular, sino adicionalmente de carácter general en materia de la circular.

Estos obviamente son temas que en algunos espacios tienden a pasar desapercibidos, porque como lo dije al principio, tienen un nivel de tecnicismo importante, pero adicionalmente, pues el tema no significa, o no tal vez tiene el mismo reconocimiento de otros que los temas nacionales llenan la agenda de lo público.

Pero doctor Amín, la importancia de este tema está referida en lo siguiente, la minería de datos ha crecido en los últimos 4 años lo que en los últimos 50 creció cualquier otro proceso industrial en el mundo.

¿Eso qué significa? Que lo que estamos viviendo en estos momentos, no solamente con el Big Data, con el Data Analytics, con el internet de

las cosas, con la inteligencia artificial, demuestran cada día más tener necesidad de actuar mucho más activamente sobre este proceso.

Yo creo que evidentemente como gobierno, aunque la Superintendencia es totalmente autónoma en esas determinaciones, avanzamos en el proceso, la discusión y estamos convencidos que la decisión fue la correcta, sin embargo, en estos momentos ni más faltaba nunca dejamos de recibir los comentarios que usted hace sobre el particular y los demás congresistas por supuesto.

Y en el segundo punto ya para terminar, usted no de ahora sino de mucho tiempo atrás, ha planteado un debate muy importante y un debate que tal vez señor Presidente no es el escenario para comentar, pero es un debate de tal magnitud que pareciera enfrentar dos derechos muy complejos, como es el derecho al buen nombre y como es el derecho a la libertad de expresión, o si ustedes lo quieren llamar como es el derecho que tiene los medios de comunicación a informar.

Ese debate que ha planteado el Senador Amín, que en algunos países se denomina el derecho al olvido, tiene mucho por desarrollar en nuestra legislación y tiene mucho por desarrollar, porque están enfrentados dos derechos de orden constitucional, que tienen igual de importancia reconocida por la Corte y que en ese test de proporcionalidad que en diferentes ocasiones la Corte hace en los análisis de sus sentencias, inclusive en algunos momentos, ha primado uno sobre el otro, pero también el otro sobre el primero.

Entonces ese ejercicio al cual usted nos está invitando a tomar decisiones sobre ese tema, pues lo aceptamos con mucho gusto y con mucha gratitud, porque son debate que bajo ninguna circunstancia se debería permitir que se marcatice, porque claro, quién no quiere, ni más faltaba que el principio constitucional de la libre expresión o el que tiene los medios de comunicación a informar no sea garantizado, no, todos estamos absolutamente consientes de esa garantía.

Pero también los ciudadanos hacen efectivos sus derechos al buen nombre y por esa razón es que la Corte Constitucional ya no en 2 sino en 3 ocasiones, y la Corte Suprema ya no en una, sino en 2 ocasiones han decidido sobre esa materia.

El Congreso es quien debe tener la potestad de regular una materia que evidentemente tiene una importancia de altísima connotación y que agradecemos Senador, pues podamos ser partícipes en esta discusión en el momento que usted lo considere o le parezca oportuno.

Y por último señor Presidente, para terminar, evidentemente, evidentemente, cada día la utilización de la red es más utilizada por los ciudadanos independientemente de su condición social, cada día la utilización de las redes sociales, pero también de los buscadores o de las formaciones más utilizadas por los ciudadanos para su información o para su opinión.

Yo en este punto quiero hacer un llamado a que seamos muy cuidadosos en cuál es esa línea, porque es una línea muy, pero muy delgada, que va de la mano evidentemente del principio de neutralidad de red, yo más que considerar el principio de neutralidad de red como un principio tecnológico lo considero como un principio democrático.

Y simplemente quiero explicarlo con un ejemplo, imaginémonos en un país cualquiera que sea, donde 1 o 2 o 3 portales opinan de manera distinta a lo que el ejecutivo está queriendo que se opine, simplemente si no existiera el principio de neutralidad, el ejecutivo tendría la posibilidad de sacar del aire entre comillas, a cualquiera de esos pronunciamientos legítimos que deben existir dentro de una democracia.

Ese principio de neutralidad de red claro que tiene unas discusiones de fondo muy, muy profundas, pero también tiene evidentemente unas connotaciones de carácter democrático que permiten desarrollar algo tan importante como es la libre discusión y la sana crítica.

En ese sentido Senador, nosotros agradecemos muchísimo la citación y esperamos obviamente señor Presidente, si es del caso contestar las preguntas o las sugerencias que haya posteriormente.

La Presidencia ofrece el uso de la palabra al doctor Daniel Arango Ángel – Viceministro de Desarrollo Empresarial encargado de las funciones del despacho del Ministerio de Comercio, Industria y Turismo:

Gracias Presidente, un saludo especial a los honorables Senadores, al Ministro de TICS David Luna y al Superintendente de Industria y Comercio Pablo Felipe Robledo, que nos acompaña el día de hoy en este importante debate.

Yo voy a tratar de ser muy breve, creo que mis compañeros de gobierno, tanto el Superintendente como el señor Ministro han explicado ampliamente las razones por las cuales se ha incluido a Estados Unidos dentro de la lista de la Superintendencia de Industria y Comercio y han hablado ampliamente sobre el marco normativo que existe en ese país y en Colombia respecto de la protección de datos.

Entonces voy hacer un breve resumen, lo primero es destacar entonces que la Ley 1581 le entrega la potestad a la Superintendencia de Industria y Comercio de proferir declaración de conformidad para la transferencia de protección de datos personales, que consecuente a esto la SIC adelantó un estudio con la firma de Valbuena Abogados, para determinar cuáles eran los países del mundo que tenían una adecuada protección de datos personales, que ese estudio si bien no incluyó a Estados Unidos como un país que digamos donde existiera según los criterios determinados por la SIC un adecuado manejo de la protección de datos.

Se colgó en la página web de la Superintendencia la circular para comentarios de los empresarios, de los ciudadanos, sobre los criterios y sobre los países que hacían buen uso de protección de datos y que como resultado de esos comentarios hubo una enorme cantidad de comentarios que se referían al respecto de la no inclusión de Estados Unidos dentro de esa lista con por supuesto argumentos que se referían a favor de que se incluyera.

Lo siguiente fue que la SIC cito a unas mesas de trabajo donde sin perjuicio de que la SIC tiene la autonomía para tomar esta decisión, se invitó al Ministerio de Comercio, Industria y Turismos, al Ministerio de las TICS y a otras entidades del Gobierno nacional y por supuesto al sector privado, a hacer parte de la discusión técnica de esas mesas de trabajo y que dentro de esas mesas de trabajo se determinó que si bien Estados Unidos no tenía una norma general que permitiera dar digamos tranquilidad en tema de protección de datos de los ciudadanos si existía todo un marco normativo con muchísimas leyes sectoriales que permitían dar tranquilidad de que efectivamente si se contaba en ese país o se cuenta en ese país con un adecuado uso y manejo de la protección de datos de los ciudadanos extranjeros y por supuesto nacionales de ese país.

Adicionalmente desatacar que a partir de ese ejercicio que se hizo en esas mesas de trabajo, la Superintendencia de Industria y Comercio tomo la decisión de incluir a los Estados Unidos dentro de la lista y destacar que como ya se ha dicho aquí ampliamente tanto por el Superintendente, como por el Ministro de las TICS, la lista no es una lista que sea cerrada, es una lista que es dinámica, es decir, que pueden entrar y salir países en cualquier momento de acuerdo al criterio que tenga la Superintendencia de Industria y Comercio en la evaluación que pueda hacer en cualquier momento.

Eso resume básicamente señor Presidente esta historia, no quiero extenderme más en comentarios adicionales, porque creo que ha sido ampliamente explicado en detalle por mis compañeros de gobierno y simplemente decirle que el Ministerio de Comercio, Industria y Comercio respalda absolutamente la decisión adoptada por la Superintendencia, gracias.

La Presidencia ofrece el uso de la palabra al doctor Nelson Remolina Angarita – Director de los Observatorios Ciro Angarita Barón de Protección de Datos y del GECTI Grupo de Estudios en Internet:

Muchísimas gracias honorables Senadoras y honorables Senadores por esta invitación y por permitirnos plantear o debatir sobre este tema que parece muy relevante.

Yo traje una presentación para mostrarles algunas cosas sobre estos puntos sobre lo que se ha dicho y lo que no se ha dicho por ahora.

Yo de entrada anticipo mi conclusión, la decisión que tomo la SIC es válida, es legítima, pero no es la mejor para las colombianas y los colombianos, es una decisión que se tomó básicamente accediendo a las pretensiones de los empresarios, pero en desmedro de los derechos de los titulares de los datos, o sea, las colombianas y los colombianos.

Quisiera plantear un poco lo siguiente, nosotros pues en la academia nos hemos dedicado a este tema, no somos los únicos que hemos trabajado el tema, desde luego sobre esto no hay un criterio de opinión.

Pero quisiera mostrarles algunos aspectos sobre las cosas que hemos trabajado, tenemos un observatorio de protección de datos donde sobre este tema hemos sido muy críticos, porque si la SIC ha tenido algo grande en sus manos es esta decisión, yo creo que todo lo que ha hecho la SIC a punta de multas es importante, pero esto que era lo más grande, me parece en mi opinión académica que no estuvo a la altura de lo que exige la Constitución nacional para proteger los derechos de las colombianas y los colombianos.

Y nosotros en la página web colocamos algunos documentos del observatorio de protección de datos para que el público conozca y acceda a muchos documentos que nos parecen importantes, bueno esto es autopropaganda del profesor Remolina, pero como tengo 5 minutos yo he escrito algunos libros sobre el tema y voy a dejarlos ahí para si algún día quieren consultarlos.

Quisiera arrancar con la carta interamericana democrática, porque en esa carta hay comas muy importantes que no hay que perder de vista y una es, en una democracia es importante la protección efectiva de los derechos y las libertades de las personas y el respeto del estado de derecho.

Yo creo que con esta norma se pone en riesgo los derechos de las personas y no se respetó el estado de derecho y un poco voy a plantear porque, cuando hablamos de transferencia internacional de datos, es como hablar de trasfusión de sangre, acá se mira que se debe hacer para no generar riesgos.

¿A quién? Al donante y al receptor de esa sangre, en datos personales se hace un ejercicio similar, aquí estamos hablando básicamente de datos de 49 millones de personas, que es muy importante tenerlo presente, y algo que me parece para tenerlo aquí claro y algo que no se ha pensado y no se ha dicho acá, es lo siguiente ¿a quién le interesa que los datos de los colombianos salgan del país? ¿Es a los ciudadanos colombianos y colombianas o es a las empresas? ¿Por qué a quién beneficia esa decisión? ¿Por qué se tomó esa decisión?

Porque si yo soy colombiano, yo puedo decidir con mi autorización envíense mis datos fuera del país, acá, perdóneme doctor Superintendente usted deicidio por 49 millones de colombianos, esa es una responsabilidad muy importante que tiene y creo que es importante que no la pierda de vista, yo en las mesas de trabajo que se citó

y en la información de la SIC que recibí, no vi representantes de ciudadanos ahí, entonces lo que yo vi principalmente en las actas que me enviaron después de un derecho de petición, es que principalmente quienes estaban allí eran representantes de empresas particularmente que les interesa básicamente que los datos de los colombiano salgan a Estados Unidos.

Es un tema de modelos de negocios en internet; y yo quiero dejar algo claro, no estoy en contra de le economía digital, ni mucho menos los modelos de negocio de las empresas, pero estas deben ser respetuosas de los derechos constitucionales y fundamentales de los ciudadanos.

La Corte Constitucional, ya lo mencionaron, dijo que no se debe perder esfuerzos de lo que hace la regulación colombiana de esa garantía de protección de los derechos de los ciudadanos cuando van a otro país, eso es lo que se llama el principio de continuidad en materia de protección de datos.

Y con fundamento en eso, pues uno mira el mapa que ya mostro el… ah ok, este es otro mapa que he elaborado, pero con fundamento en información – información, pues desde luego en todas partes del mundo no se protege los datos personales de la misma manera, ni es pretensioso que ello sea así, pero si hay que buscar que tenga por lo menos unos mínimos, aquí hay que mirar si Estados Unidos en ese listado tiene esos mínimos.

Como otros países que ustedes ven en blanco, el tema de porque se centra el debate en Estados Unidos es porque básicamente Colombia es el único país del mundo que ha dicho que Estados Unidos si tiene nivel adecuado de protección de datos, entonces es muy curioso, otros países ya han dicho que no, han llegado a algunas medidas o acuerdos para que se envíen datos a Estados Unidos, pero no desde cualquier manera y eso también es importante tenerlo presente.

Aquí ustedes ven en documentos internacionales, cuales son las medidas que existen para transferir datos internacionales o a transferencias internacionales de datos, esto es exportar datos y son muchas, no solo es un tema de nivel adecuado de protección, una de las críticas a la decisión de la SIC es que solo pensó en esa, el tema de la responsabilidad demostrada no está ahí ¿pero por qué no incluirla? La responsabilidad demostrada como voy a plantearles y como está actualmente en Colombia es un concepto muy gaseoso, decir, que debemos ser responsables, eso ya lo sabemos hace muchos siglos por favor, aquí debemos adoptar una medida preventiva para que los derechos de los ciudadanos no asuman riesgos.

La mejor forma de proteger un derecho constitucional fundamental es evitar su vulneración, no debemos esperar que haya vulneración y entonces ahí si empezar a actuar, no, aquí una medida más sensata y responsable con los derechos de los ciudadanos, es evitar la vulneración y yo veo que aquí en la decisión de la SIC no hay medidas en ese sentido, eso es algo muy importante.

Entonces quiero que tengan por favor presente que hay muchas formas para transferir datos a Estados Unidos y a cualquier otro país del mundo, y también algo clave, yo no es que esté hablando de que no se deben transferirse datos a ningún país del mundo, por favor, eso es algo que es inevitable, me parece necesario, pero lo que si estoy en desacuerdo es que se haga de la manera como lo dijo la SIC.

En eso sí me parece que la SIC debió pensar más en los derechos de los colombianos y las colombianas y no en los intereses de algunas empresas y de prevalecer los modelos de negocios de algunas empresas en internet.

Esa es mi visión sobre el tema, por favor, el Superintendente planteaba que hay en Estados Unidos, porque la misma norma nuestra habla de que ese país de destino no debe tener un nivel de protección inferior al que otorga la ley colombiana, bueno, ahí hay un cuadro señor Superintendente, que usted puede ver que efectivamente en Estados Unidos no es ni igual, ni superior al colombiano.

Primero, allá el tema no es un tema de un derecho constitucional fundamental como sí lo es en Colombia, allá no tenemos una ley general, allá no hay una autoridad de protección de datos general para todo tipo de datos, desde luego, hay normas sectoriales, pero no aborda todos los datos.

Unas de las preguntas que vi en el cuestionario, pues se le preguntaba a la Superintendencia, bueno muéstreme todas las normas que cubran todos los datos y si eso es igual como sucede en Colombia en cuanto a los deberes que tiene los responsable encargados de datos, miren la respuesta y la repuesta es muy general, o sea, hay normas, hay derechos y hay deberes, pero lo que se busca es mirar si esas garantizan un nivel igual o similar al colombiano, ese ejercicio, por lo menos en la respuesta no se hizo.

Lo único que coinciden Colombia y Estados Unidos es en que tiene normas sectoriales y eso es muy, muy importante, por ejemplo, mecanismos efectivos de protección de datos, en Estados Unidos no existe la acción de tutela, como sí aquí, para que un colombiano si hay una violación de sus derechos constitucionales fundamentales como es la protección de datos lo haga, aquí sí, allá no.

En Colombia el tratamiento indebido de datos es tan delicado y ha habido tanta responsabilidad del regulador, que incluso hay un delito de violación de datos personales, en Estados Unidos no hay ese tema.

Tenemos un mecanismo de consultas y reclamos, artículo 14 y 15 de la ley, que da unos temas específicos y muy puntuales, la SIC ha sancionado empresas porque no encuentran esos

términos, por ejemplo, eso no existe en Estados Unidos, los términos son diferentes.

Entonces yo quiero dejar claro que aquí estamos enviando datos a un país que tiene otro nivel de protección, pero no igual o superior al colombiano y la norma dice que uno no debe enviar datos a un país que tenga niveles inferiores. Entonces me parece relevante tener presente ese aspecto.

Pero además del marco jurídico, cuando se envían datos de colombianos a cualquier país se asume riesgo político, porque hay que mirar quién está en ese país allá, qué tipo de país es, qué democracia, si es una democracia o no y qué decisiones se están tomando.

Bueno, la noticia este año, que me parece importante es las políticas que ha adopta el Presidente Donald Trump respecto de la protección de datos de extranjeros.

Miren por favor esas noticias de EL Tiempo, son de febrero de este año y hay un poco básicamente lo que está planteando es que la privacidad para extranjeros desaparece para ciertas cuestiones, eso es algo importante para tener presente, no solo miremos normas, sino a donde estamos enviando, que va pasar con los datos de los ciudadanos allá, eso es relevante y precisamente este tema ha generado…

…Pero, aunque veo, esta preocupación no solo es de profesores, ni nada, sino de asociaciones de protección de derechos humanos, de los mismos Estados Unidos, ahí hay una carta precisamente de la Asociación Americana de Derechos, quejándose ante el mismo gobierno de Estados Unidos y también otras ante las autoridades europeas, sobre las decisiones del presidente Donald Trump en este tema. Entonces mírese en el riesgo político también de que pasa los datos allá.

Otro tema y ya lo plantea el doctor Amín, es que hay académicos también muy serios que han dicho es que eso es así, ahí está un estudio también y conclusiones de la Universidad de Harvard en ese tema, entonces yo creo que es importante mirar esos elementos.

Aquí en cambio veo importante un cambio de un género copernicano que he llamado de febrero a mayo la SIC, en un primer momento dijo Estados Unidos no tiene nivel adecuado y en el otro momento dijo sí, sin mayores cambios en la misma decisión, en los motivos.

Aquí quiero llamar la atención lo siguiente, la SIC, en menos de 7 meses considero que más de 44 países del mundo tiene nivel adecuado de protección, previo a eso la SIC cuando la pidieron que se manifestara solo sobre un país, Alemania, que es el país que en este tema se considera el más duro en protección de datos, se gastó 19 meses, yo veo como que hubo mucha agilidad, fue muy expedito, pero realmente lo que yo percibo que lo que hubo fue eso, pero poco estudio en el tema.

El tema de la decisión de la SIC es si el fin justifica los medios, aquí por favor, enviar datos a Estados Unidos, desde luego que sí, ¿pero de cualquier manera? ¿A cualquier costo? Y que pensamos de los derechos de los ciudadanos y sobre esto la Corte Constitucional ya en muchas sentencias ha hablado de los juicios de proporcionalidad, ahí dice cuando se toma una medida que afecta derechos constitucionales fundamentales, hay que mirar si primero esa medida tiene un fin constitucional legítimo, no lo encuentro en esta circular cual es el fin constitucional legítimo, seguramente lo hay.

Si esa medida sirve para lograr esa finalidad, uno diría sí, sí esa medida era necesaria, es decir, si no existen otras alternativas.

La Presidencia ofrece el uso de la palabra al doctor Antonio Medina Gómez – Director del ACUI:

Buenos días, gracias señor Presidente, señores Senadores, señor Ministro, señor Superintendente de Industria y Comercio por permitirnos participar en este debate público.

Esta mañana al comenzar el debate yo escuchaba al doctor Amín y veía que hacía referencia a la ley de protección de datos personales y al hábeas data en un escenario de años atrás, toda una experiencia institucional, académica y por supuesto política sobre estos temas.

Es preocupante, a pesar de que encontramos posiciones distintas como la del Senador Amín explicando un poco una situación que requiere la atención de los colombianos en esta materia y la explicación que da el Superintendente de Industria y Comercio muy razonable y muy sólida como para uno decir estoy en un escenario en que no se a quien se le debe dar la razón.

El Ministro Luna tocó un punto muy importante en su intervención, del cual me parece importante mencionarlo y recordarlo y es que se está ahorita en Cartagena se creó el Viceministerio de Economía Digital, estamos dando pasos hacia esa nueva economía, hoy se estaba hablando de internet de las cosas, se está hablando de Big Data, se está hablando de ciudades inteligentes y todo esto propone el tener los ojos y la mente concentrados en la adecuada protección de datos de los colombianos en internet.

Ayer anunciaron un internet mucho más veloz, mucho más ágil, que es el internet cuántico, que se ve aquí a minutos, entonces la pregunta es hacia a donde tenemos que mirar, yo creo ¿que la preocupación es Estados Unidos? ¿La preocupación son algunas empresas? Hoy hay muchas empresas que están capturando información de los colombianos y ni siquiera nos estamos dando cuenta.

¿Cómo hace la Superintendencia de Industria y comercio? Yo no sé si existe un procedimiento en donde una empresa se acerca a la Superintendencia

y le dice: mire yo estoy administrando una base de datos, la vamos a llevar a Estados Unidos o a un servidor y esto es lo que vamos hacer, no conozco ese procedimiento y no sé si es claro y tampoco conocemos si los colombianos efectivamente están dando un consentimiento sobre quien tiene la responsabilidad de esos datos, si es en Colombia o si los llevan en la nube.

Hoy a través de internet podemos con un solo clic transmitir información, bases de datos, archivos, no solamente a un país, lo podemos transmitir a 100 países simultáneamente, ¿entonces en donde está la responsabilidad? y ¿dónde están las acciones serias del gobierno colombiano, de la autoridad que es la Superintendencia de Industria y Comercio para velar por la efectiva protección de los datos personales de los colombianos?

Yo creo que esa es la preocupación desde la Asociación Colombiana o Usuarios de Internet y es velar porque haya una transparencia en ese tipo de procesos, que los colombianos sepamos exactamente cuál es el nivel de responsabilidad de cada una de las compañías en esa materia.

Por mencionarlo, estamos organizando un taller y nos estamos dando cuenta en la planeación de ese taller, que hay uno de los puntos esenciales que se llama la confianza de los ciudadanos a las empresas en las cuales le depositan esos datos y les confían esa información.

Muchas veces no hay una garantía, no hay un contrato que hable de eso, pero la confianza que el colombiano deposita en su entidad financiera, en la universidad, en una compañía de seguros, en una aerolínea, en un hotel, en donde se registre y este dejando información.

Entonces la confianza también se debe valorar en este propósito.

No quise ser amplio, no quise hacer ninguna presentación, sencillamente manifestarles que para nosotros es muy importante que efectivamente lo que se decida aquí en esta reunión, las decisiones que tome la Superintendencia estén orientadas efectivamente a informar adecuadamente a los colombianos sobre todo lo que le concierne el alcance de esas decisiones en materia de protección de datos personales, en el ámbito de esta nueva economía digital que es un poco todavía oscura y está por definirse.

Muchas empresas en Colombia están en una carrera agitada, rápida, de ingresar a esa nueva economía digital independiente de que acciones van a tomar, deben considerar dentro de sus planes estratégicos el preservar, conservar, proteger, la información de los colombianos en internet.

Internet es una red portentosa, ágil, veloz y los servicios y contenidos en internet están de alguna manera facilitando esa captura de información de los colombianos.

Hasta aquí, les agradezco la invitación, muchas gracias.

La Presidencia ofrece el uso de la palabra al doctor Andrés Umaña Chaux – Representante de Colombia Microsoft:

Buenas tardes señor Presidente y muchas gracias a los honorables Senadores y Senadoras por la invitación a participar en este foro.

1. Yo quisiera simplemente hacer 3 comentarios muy rápidos.
2. Como lo han manifestado el señor Superintendente, el señor Ministro y el honorable Senador Amín, celebramos la realización de este debate, en una época en la que estamos hablando de transformación digital, de utilizar los sistemas de información para nuestros compromisos, para el cumplimiento de las funciones públicas, es fundamental tener este debate, el manejo de la información se vuelve el elemento fundamental y en esa medida la regulación de cómo se maneja esa información es muy importante.

Cuando ustedes piensen en Inteligencia Artificial, en Big Data, en internet de las cosas, todos estos fenómenos tecnológicos de una u otra manera como lo mencionaba el Senador y el profesor Remolina involucran un mayor manejo de la información, y las empresas claro que si están captando mucha más información que las que antes captaban en relación con los ciudadanos.

Y en esa medida un sistema de protección de la información es fundamental, pero yo quería referirme a un comentario que hizo el profesor Remolina en el sentido de que esta decisión era solo para defender un modelo de negocio, no se trata de defender un modelo de negocio de las empresas, obviamente las empresas tienen un interés comercial, pero es el acceso a este tipo de tecnologías lo que está en juego.

Las herramientas de inteligencia artificial y las herramientas de internet de las cosas, no están en Colombia, están provistas muchas veces por empresas en otros países y por eso es fundamental tener un adecuado balance como lo mencionaba el Ministro Luna entre la protección de los ciudadanos y la posibilidad de que haya un libre flujo de información hacia otros países.

Nosotros como compañía estamos totalmente prestos a acudir a cualquier debate que se haga, usted sabe Senador Amín, hemos estado en todas las mesas de discusión a las que nos han invitado, hemos hecho propuestas y la invitación que hacemos frente a este tema es que debe ser una, como lo hemos discutido también en esas mesas de trabajo, es que esto debe tratarse como un problema integral, no estamos solamente hablando de un tema de transferencia internacional de datos, sino que efectivamente como se protegen los derechos de los ciudadanos.

Nosotros las empresas, o por lo menos hablo digamos por Microsoft como compañía, estamos interesados en competir en como mejor

protegemos la información de los ciudadanos, somos conscientes de la importancia que tiene la protección de la información para cada uno de los colombianos y en esa medida nosotros como compañía debemos competir no solamente por nuestros productos y servicios, sino por proteger cada vez más a los ciudadanos, eso es un diferencial en el mercado que inclusive nos va generar una sana competencia para proteger la privacidad y generar ese objetivo que creo que todos estamos buscando acá.

Pero el mensaje que quería dejar también Senador Amín, que lo hemos discutido es que esto es un problema transfronterizo de servicios que como tal también exige herramientas de comercio transfronterizo de servicios, yo muchas veces extraño en estas discusiones ejemplos o herramientas de cómo el gobierno colombiano por ejemplo puede ejecutar sus decisiones, nosotros nunca hemos tenido creo, al Ministerio de Relaciones Exteriores por ejemplo dándonos una explicación de cómo funcionan esos mecanismos de ejecución de decisiones administrativas y judiciales en otros países.

Y cuando yo pienso en cómo se deben solucionar estos problemas y estas necesidades que usted muy bien plantea, creo que parte de la respuesta está en eso, una solución internacional en donde haya cooperación internacional entre las autoridades, en donde haya mecanismos idóneos, jurídicos para la cooperación entre las autoridades.

En este momento se discuten en este Congreso como usted lo sabe la aprobación del convenio contra la lucha contra el cibercrimen, no me voy a pronunciar sobre las bondades o si es bueno o malo, pero ese es un ejemplo de cómo hay instrumentos internacionales que permiten generar herramientas efectivas para proteger los derechos de los ciudadanos en internet.

Finalmente, quería simplemente terminar nuevamente por agradecer a las autoridades, a la Superintendencia, al Ministerio, al Congreso de la República, a usted Senador Amín por los debates que hemos tenido en relación con este tema, ustedes saben que llevamos pues meses trabajando, nosotros directamente como compañía y a través de nuestros gremios, de la ANDI, de la CCIT, de la Cámara Colombiana de Comercio Electrónico, hemos participado activamente y lo seguiremos haciendo.

Y coincidimos en que debemos seguir trabajando en estos temas para lograr ese balance del que todos hemos hablado aquí en este foro el día de hoy, muchas gracias.

La Presidencia ofrece el uso de la palabra a la doctora Sandra Pascua – Vicepresidente Cámara Colombiana de Informática y Telecomunicaciones:

Bueno, buenas tardes a todos, muchísimas gracias por la invitación, quiero en primer lugar excusar al doctor Alberto Samuel Yohai, desafortunadamente se le cruzo la agenda y no pudo participar en este importante debate, para nosotros la CCIT es muy importante el tema de protección de datos personales y por eso siempre hemos estado de manera activa participando no solo en todos los debates, sino en los trámites de los proyectos de ley y obviamente en el procedimiento de expedición de la Circular 005 de la Superintendencia de Industria y Comercio.

Nosotros como CCIT y nuestras empresas afiliadas, obviamente la protección de datos es muy importante, es algo esencial, las empresas nuestras son responsables en el manejo de estos datos y por eso cuando la Superintendencia de Industria y Comercio expidió el primer borrador de circular, pues nosotros hicimos parte activa, no solo de los comentarios que enviamos, sino de la mesas de trabajo que menciono el señor Superintendente para poder hacer ajustes a la circular, velando por la protección de los datos personales, no se afectara el tema de la transformación digital y la economía digital del país.

Nosotros dentro de los comentarios manifestamos la importancia de que el uso de los servicios tecnológicos que implican el movimiento transfronterizo de información como el cloud computing y el comercio móvil y el internet de las cosas, ha permitido entre otros la aparición de una nueva eficiencia global y un nuevo 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, además no podemos olvidar que el 70 por ciento el negocio global de hosting se desarrolla en Estados Unidos y por eso uno de los comentarios que nosotros enviamos a la Superintendencia de Industria y Comercio fue la necesidad de incluir Estados Unidos dentro de la lista.

No solo solicitamos la inclusión de Estados Unidos, sino también de otros países como Brasil y como Ecuador y soportamos nuestras solicitudes en las diferentes normas de protección de datos, e instituciones de protección de datos que aquellos países tienen, que, si bien no son una norma general o no son exactamente iguales a la colombiana, pues si consideramos que de todos modos velan por estar protección de datos.

Pero nosotros por eso consideramos que de las propuestas regulatorias que se expidan, deben velar por promover la interoperabilidad de las normas de protección de datos y con ello hacer que los procesos administrativos automatizados sean seguros para que los usuarios estén protegidos.

Por eso respetuosamente nosotros respetuosamente le sugerimos en su momento al Superintendente que se creara un sistema que permitiera esa flexibilidad y esa interoperabilidad

entre países para permitir esa transferencia de datos personales.

Nosotros celebramos que la Superintendencia de Industria y Comercio incluyo a Estados Unidos dentro de la lista y como usted lo sabe Senador Amín la CCIT siempre ha estado preocupada por este tema y usted muy amablemente siempre nos ha abierto la puerta para poder presentarle nuestros comentarios, incluso al proyecto de ley modificatoria de la Ley 1581 en el cual la CCIT le envió también comentarios y hemos siempre estado como con esa disposición, no solamente en la parte de protección de datos, sino que también el comercio y la economía digital fluyan en el país.

Y que los datos de los colombianos que vayan a ser transferidos o mediante contratos de transmisión, pues de todos modos tengan la protección debida, porque ese un tema que le importa mucho a la CCIT.

Entonces pues nosotros si le argumentamos al señor superintendente no solo con la cantidad de normas que el leyó hoy sobre las normas que existen en los Estados Unidos, sino que también hay reportes y estudios que han declaro el régimen de privacidad de los Estados Unidos como esencialmente equivalente al de la Unión Europea, y la misma Corte Europea de Justicia ha reconocido adecuado los mecanismos y estándares que tienen Estados Unidos para le protección de la información de las personas.

Entonces nosotros como CCIT si bien queremos ser partícipes activamente en todos los proyectos y toda la normatividad que esté orientada a la protección de datos, porque es un tema de gran importancia para nuestras empresas, no solo porque obviamente pues también son sus clientes, porque velan por su seguridad, porque velan por su protección, pero también es necesario que se pueda sacar adelante todos los temas de la transformación y la economía digital.

Y por eso también queremos poder tener participación en el trámite del proyecto de ley que se está en discusión hoy precisamente en esta comisión, para que podamos como lo dijo el señor Ministro de TIC participar en esas mesas de trabajo a fin de sacar una normatividad que…

…No, simplemente para que ajustando la Ley 1581, de las normas internacionales podamos tener ese escenario de protección de datos, por un lado, y transformación y economía digital por el otro.

Muchísimas gracias por su atención.

La Presidencia ofrece el uso de la palabra al doctor Mauricio López – Directivo Andesco:

Buenos días honorables Senadores, señor Presidente, señor Ministro, señor Superintendente, señor Ministro encargado de Comercio, Senador Amín, muchísimas gracias por permitirnos participar en este importante debate sobre un tema sustancial para los colombianos cual es la protección de datos.

Creo que el primer punto de referencia es que apenas los colombianos estamos dándonos cuenta que hay que proteger los datos, yo creo que ese es el principal reto y esfuerzo que hay que seguir trabajando duro.

Es un trabajo que ha sido arduo para cambiar una cultura, una civilización, hay que empezar por las abuelas decía Víctor Hugo, lo cual significa que son por las menos 2 generaciones continuas para trabajar en ello.

Y por lo tanto entonces el trabajo que hace la Superintendencia de Industria y Comercio es un trabajo arduo, difícil, por una sencilla razón además en este tema, por la extraterritorialidad, porque si fuera fácil el control sobre los datos acá en Colombia y no tema como el nuestro en donde el internet y la economía es extraterritorial terse, les va ser mucho más complicado.

Yo creo que ese es un gran reto y es el gran esfuerzo que hace la superintendencia diariamente para poder acopiar dentro de su margen de normativa y sobre todo esquemas y protocolos de verificación, inspección y vigilancia, lograr tener el tema.

Por eso la disponibilidad entre las leyes de privacidad nacional y las prácticas internacionales que se han desarrollado en el ecosistema e internet, plantean las dificultades también para los operadores de servicio, porque como el internet se va a través de los operadores de servicios, los datos van a través de la red de los operadores, pues allí siempre podrá caer la tentación de que sean los operadores los responsables del manejo de datos per se y es un tema que siempre hay que tener de cuidado.

Por eso tales deferencias asentadas en la extraterritorialidad pueden provocar incertidumbre entre los operadores, por eso el principio de mismos servicios, mismas reglas y misma protección debe ser el elemento básico que sustente el desarrollo de la regulación para la economía digital.

Las precauciones que se adapten en este sentido deben ser el resultado de una combinación de enfoques acordados, tanto a nivel internacional, como también en la legislación del país nuestro, Colombia, y por supuesto de las medidas que adopten los operadores, en nuestro caso los afiliados a Andesco, pero también los proveedores de contenidos, etc.

Y en ese orden de ideas es muy breve lo que vamos a terminar, es importante señalar acá que hay agentes que no tienen presencia en Colombia y es válido, porque la extraterritorialidad y la tecnología de la información y las comunicaciones aplanaron la tierra y por lo tanto el mundo es una gran haya global en los temas de las TICS.

Pero sí proveen los servicios en Colombia y sí recolectan y tratan datos de colombianos para fines comerciales, por lo tanto es importante y este es el mensaje, es un gran esfuerzo y en eso acompañaremos al gobierno nacional como lo hemos acompañado siempre y al Congreso de la República en buscar las mejores hormas posibles para que sin pretender cambiar la tendencia mundial, que es ese mundo global en el tema de las tecnologías de la información y las comunicaciones, si podamos tener una confianza en que los datos de los colombianos realmente sean protegidos.

Y lo mejor, que cuando sean eventualmente violentados tengamos la posibilidad de poder acceder a las instancias pertinentes para su adecuada protección.

Por eso señores Senadores esa era nuestra intervención, acompañamos estos procesos, no es fácil, en este mundo de la globalización estos temas serán muy difíciles y un mensaje final, creo que sería importante incentivar a los colombianos que cada vez que carguemos una app sea muy amplio el tema del acepto, para indicar que cuando yo acepto para poder bajar la app quede muy claro lo que yo estoy indicando con ese acepto.

Pareciera tonto lo que yo estoy diciendo, pero creo que muchas veces la app que bajamos, todos los que bajamos apps todos los días no nos estamos dando cuenta que cuando estamos dando el acepto ya *per se* estamos dejando una ventana de opción, entonces tiene que haber pisado un mensaje también de mayor publicidad en eso para que los colombianos y la ciudadanía en general tenga en cuenta esos elementos.

Eso era lo que queríamos decir señor Senador, muchas gracias señor Presidente y señores Ministros y Superintendente, muchísimas gracias.

La Presidencia concede el uso de la palabra al citante honorable Senador Jaime Amín Hernández:

Gracias Presidente, voy hacer unas muy breves conclusiones de este debate que como ha quedado, claro aún nos sigue generando más preguntas que respuestas, y quiero decirle al Superintendente lo siguiente, en lo personal valoro el carácter con el que usted ha asumido la defensa y la protección de los consumidores en Colombia, ha dado batallas muy importantes, se lo digo de una manera conclusiva y personal.

Pero me preocupa señor Superintendente una frase que usted dijo y la digo además de una manera muy aplomada, no la dijo al desgaire, usted dijo palabras más, palabras menos, que con esa decisión de la Circular 05 del 2017 con relación a la transferencia de datos hacia los Estados Unidos, ustedes, hablo del gobierno pudieron haber acertado o se pudieron haber equivocado.

Y eso dicho en cabeza del órgano rector de la protección de datos de los colombianos me parece muy delicado, muy grave, con unas enormes implicaciones para la seguridad de la defensa de los derechos fundamentales de los colombianos.

En particular este que estamos abordando en el tema del hábeas data, que lo diga un Senador de la oposición o del gobierno vaya y venga, pero que las palabras provengan precisamente de quien debe dar fe del cuidado, de la protección y del alcance de estas decisiones que ustedes han tomado, me parece bastante delicado doctor Robledo.

Agradezco también al Ministro Luna, la disposición que muestra frente a… no solo al tema del debate del día de hoy, si no de la norma que hemos venido trabajando con los compañeros del partido y que ya fue aprobada en esta comisión en la legislatura anterior, de manera unánime, 15 votos a favor, 0 en contra.

Que es aquella que quiero venderles la idea porque vamos a insistir en ello, ya está presente en el Orden del Día de esta comisión como ley estatutaria, y es aquella que busca repito proteger los derechos de los consumidores colombianos de internet frente a empresas que operando en Colombia no tienen domicilio en Colombia.

Creo que es un tremendo paso, como diría Neil Armstrong cuando lo entrevistaron allá en la luna, un pequeño primer paso, pequeño primer gran paso que demos desde la legislación para proteger los derechos de los consumidores colombianos en el internet.

Y a manera de conclusión sí quisiera destacar algunos datos que ha dado el profesor Remolina, sin duda, sin duda queda claro que la SIC tomo la Superintendencia tomo la decisión de certificar a Estados Unidos como un país protector de datos.

Y eso será una responsabilidad que ha compasada esa con la frase esa del Superintendente me deja más inquietudes y preocupaciones que respuestas.

Lo segundo, no es cierto como lo afirmo la Superintendencia en las repuestas al cuestionario que Europa declaro que Estados Unidos tiene un nivel de protección adecuado de datos, como país, no es Estados Unidos como país, es algunas empresas de los Estados Unidos que si tienen un nivel adecuado de protección de datos y por tanto Europa permite que sus datos traspasen a los Estados Unidos.

Lo tercero tal vez es el almendrón del debate y es que tampoco la Superintendencia respondió de manera juiciosa y de fondo a la pregunta perdón del cuestionario, la numero 10 en particular, donde en desarrollo de lo que dijo la Corte Constitucional cualquier decisión, de cualquier autoridad, legislativa o gubernativa de Colombia, no puede en materia de protección de datos, para que los datos de los colombianos sean exportados

hacerse a una legislación cuyo nivel de protección sea inferior a la del gobierno colombiano, la de los ciudadanos colombianos.

Y tengo que recordar también que precisamente cuando se expidió la 1581 señor Superintendente, lo que se buscaba era que con la expedición de esa ley y de esa normativa a Colombia se le tuviera como un país que, en el concierto de naciones, internacionalmente hablando de protección de datos, le daba valoración muy alta al sistema de protección del buen nombre de los ciudadanos colombianos.

Lo otro, que también queda claro que, en materia de protección de datos, mientras que el artículo 15 de la Constitución consagra como un derecho fundamental el derecho al buen nombre de los colombianos, esta tratativa no tiene el mismo rango en los Estados Unidos, no hay una protección de orden constitucional o elevada al nivel de una de las 26 enmiendas de la Constitución de los Estados Unidos, sino que se hace una, como bien lo dijo el Superintendente, una protección sectorial, por eso usted hace alusión a las diferentes autoridades de protección, en materia de comercio, de salud, etc. Que hay en los Estados Unidos.

Pero no a nivel federal como existe por ejemplo aquí en todo el territorio colombiano con la Superintendencia de Industria y Comercio.

Y, por último, creo que con este paso que bien valdría la pena señor Superintendente y ministro que revisaran, la decisión de la SIC pone en riesgo que Europa declare que en la legislación colombiana sean relajados por decirlo de alguna manera, los niveles adecuados de protección de datos de los ciudadanos colombianos.

Porque si de Europa trasladaban datos con base en la 1581 y certificado en que Colombia era un país que tenía un nivel adecuado de protección de datos, con esta circular se está borrando con la mano izquierda lo que se escribió con la mano derecha.

De tal suerte que Europa puede en adelante concluir que los datos que de Europa se trasladen a Colombia podrán ser re exportados hacia los Estados Unidos sin un nivel adecuado de protección de datos por cuenta de la resolución, la circular expedida por la Superintendencia de Industria y Comercio.

Entonces cierro este debate o esta intervención señor Presidente dando clara muestra de que a nuestro juicio y en un contexto de diría yo, mayores y menores implicaciones, con la decisión de la circular, de la Superintendencia de Industria y Comercio, evidentemente los colombianos no podremos hacia el futuro dormir tranquilos porque estaremos expuestos a que todo tipo de datos y no solamente aquellos relacionados con el comercio, hoy la industria serán expuestos y traficados sin un nivel adecuado de protección conforme lo registra y lo prescribe el artículo 15 de la carta política. Muchas gracias señor Presidente.

Atendiendo instrucciones de la Presidencia por Secretaria se da lectura a los proyectos que por su disposición se someterán a discusión y votación en la próxima sesión ordinaria:

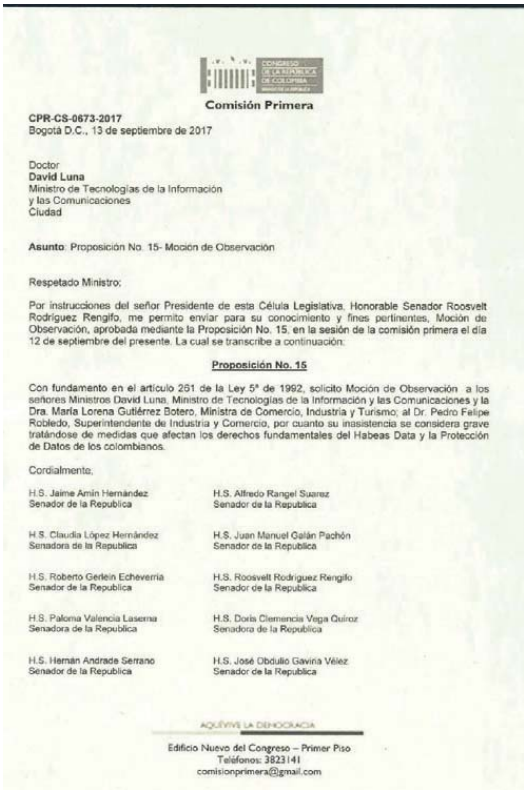
1. **Proyecto de ley número 89 de 2017 Senado,** *por medio de la cual se modifica la Ley Estatutaria 1581 de 2012*.
2. **Proyecto de Acto Legislativo número 13 de 2017 Senado, 265 de 2017 Cámara,** *por medio del cual se modifican los artículos 186, 234 y 235 de la Constitución Política y se implementa el derecho a la doble instancia y a impugnar la primea sentencia condenatoria*. (Doble Instancia).
3. **Proyecto de ley número 106 de 2017 Senado, 263 de 2017 Cámara,** *por el cual se establece el procedimiento de pérdida de la investidura de los Congresistas, se consagra la doble instancia, el término de caducidad, entre otras disposiciones*.
4. **Proyecto de ley número 30 de 2017 Senado,** *por medio de la cual se modifica el Decreto-ley 888 de 2017*.
5. **Proyecto de ley número 20 de 2017 Senado,** *por medio de la cual se reforma el Decreto 1421 de 1993 en relación con la remuneración de los Alcaldes Locales y los Ediles de Bogotá*.
6. **Proyecto de ley número 34 de 2017 Senado,** *por medio del cual se fortalece el ejercicio funcional de las Personerías Municipales*.
7. **Proyecto de ley número 32 de 2017 Senado,** *por medio del cual se modifica el Decreto 903 del 29 de mayo de 2017 y se dictan otras disposiciones*.
8. **Proyecto de Acto Legislativo número 03 de 2017 Senado,** *por medio del cual se reforma la Constitución Política de Colombia en lo relativo a la remuneración de los miembros del Congreso de la República*.
9. **Proyecto de ley número 255 de 2017 Senado, 090 de 2016 Cámara,** *por medio de la cual se modifica el artículo 1025 del Código Civil*. (Indignidad Sucesoral).
10. **Proyecto de Acto Legislativo número 02 de 2017 Senado,** *por medio del cual se modifican los artículos 328 y 356 de la Constitución Política de Colombia*. (Distrito Especial a San Miguel de Agreda de Mocoa).
11. **Proyecto de ley número 14 de 2017 Senado,** *por medio de la cual se fortalece la política criminal y penitenciaria en Colombia y se dictan otras disposiciones*.

VII

Negocios sustanciados por la Presidencia

Anexo N° 1

Moción de Observación: Doctor David Luna Sánchez - Ministro de Tecnologías de la información y las comunicaciones; doctora María Lorena Gutiérrez Botero – Ministra de Comercio, Industrial y Turismo; doctor Pablo Felipe Robledo – Superintendente de Industria y Comercio.



Comisión Primera

CPR-CS-0673-2017
Bogotá D.C., 13 de septiembre de 2017

Doctor
David Luna
Ministro de Tecnologías de la Información
y las Comunicaciones
Ciudad

Asunto: Proposición No. 15- Moción de Observación

Respetado Ministro:

Por instrucciones del señor Presidente de esta Célula Legislativa, Honorable Senador Roosvelt Rodriguez Rengifo, me permito enviar para su conocimiento y fines pertinentes, Moción de Observación, aprobada mediante la Proposición No. 15, en la sesión de la comisión primera el día 12 de septiembre del presente. La cual se transcribe a continuación:

Proposición No. 15

Con fundamento en el artículo 251 de la Ley 5ª de 1992, solicito Moción de Observación a los señores Ministros David Luna, Ministro de Tecnologías de la Información y las Comunicaciones y la Dra. María Lorena Gutiérrez Botero, Ministra de Comercio, Industria y Turismo; al Dr. Pedro Felipe Robledo, Superintendente de Industria y Comercio, por cuanto su inasistencia se considera grave tratándose de medidas que afectan los derechos fundamentales del Habeas Data y la Protección de Datos de los colombianos.

Cordialmente,

H.S. Jaime Amín Hernández
Senador de la Republica

H.S. Alfredo Rangel Suarez
Senador de la Republica

H.S. Claudia López Hernández
Senadora de la Republica

H.S. Juan Manuel Galán Pachón
Senador de la Republica

H.S. Roberto Gerlein Echeverria
Senador de la Republica

H.S. Roosvelt Rodriguez Rengifo
Senador de la Republica

H.S. Paloma Valencia Laserna
Senadora de la Republica

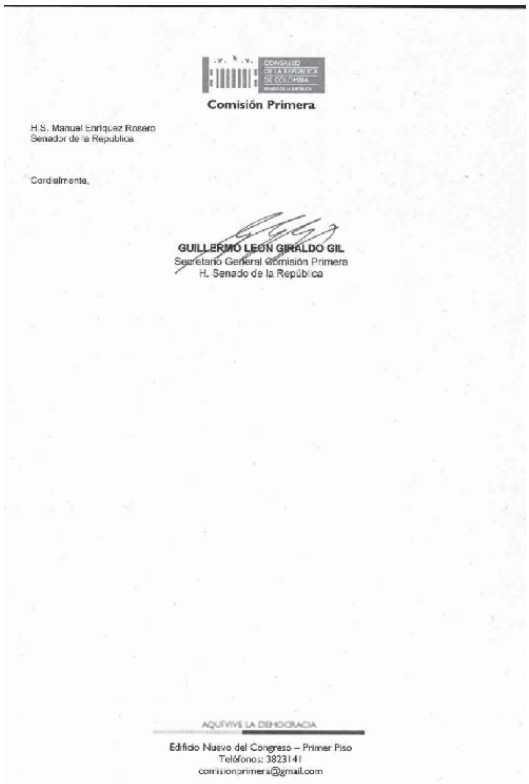
H.S. Doris Clemencia Vega Quiroz
Senadora de la Republica

H.S. Hernán Andrade Serrano
Senador de la Republica

H.S. José Obdulio Gaviria Vélez
Senador de la Republica

AQUÍ VIVE LA DEMOCRACIA

Edificio Nuevo del Congreso – Primer Piso
Teléfonos: 3823141
comisionprimera@gmail.com



Comisión Primera

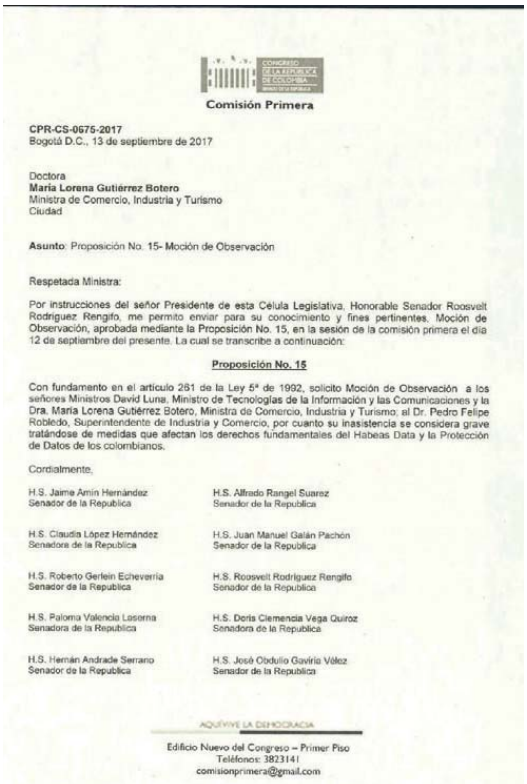
H.S. Manuel Enriquez Rosero
Senador de la Republica

Cordialmente,

GUILLERMO LEON GIRALDO GIL
Secretario General Comisión Primera
H. Senado de la República

AQUÍ VIVE LA DEMOCRACIA

Edificio Nuevo del Congreso – Primer Piso
Teléfonos: 3823141
comisionprimera@gmail.com



Comisión Primera

CPR-CS-0675-2017
Bogotá D.C., 13 de septiembre de 2017

Doctora
María Lorena Gutiérrez Botero
Ministra de Comercio, Industria y Turismo
Ciudad

Asunto: Proposición No. 15- Moción de Observación

Respetada Ministra:

Por instrucciones del señor Presidente de esta Célula Legislativa, Honorable Senador Roosvelt Rodriguez Rengifo, me permito enviar para su conocimiento y fines pertinentes, Moción de Observación, aprobada mediante la Proposición No. 15, en la sesión de la comisión primera el día 12 de septiembre del presente. La cual se transcribe a continuación:

Proposición No. 15

Con fundamento en el artículo 251 de la Ley 5ª de 1992, solicito Moción de Observación a los señores Ministros David Luna, Ministro de Tecnologías de la Información y las Comunicaciones y la Dra. María Lorena Gutiérrez Botero, Ministra de Comercio, Industria y Turismo; al Dr. Pedro Felipe Robledo, Superintendente de Industria y Comercio, por cuanto su inasistencia se considera grave tratándose de medidas que afectan los derechos fundamentales del Habeas Data y la Protección de Datos de los colombianos.

Cordialmente,

H.S. Jaime Amín Hernández
Senador de la Republica

H.S. Alfredo Rangel Suarez
Senador de la Republica

H.S. Claudia López Hernández
Senadora de la Republica

H.S. Juan Manuel Galán Pachón
Senador de la Republica

H.S. Roberto Gerlein Echeverria
Senador de la Republica

H.S. Roosvelt Rodriguez Rengifo
Senador de la Republica

H.S. Paloma Valencia Laserna
Senadora de la Republica

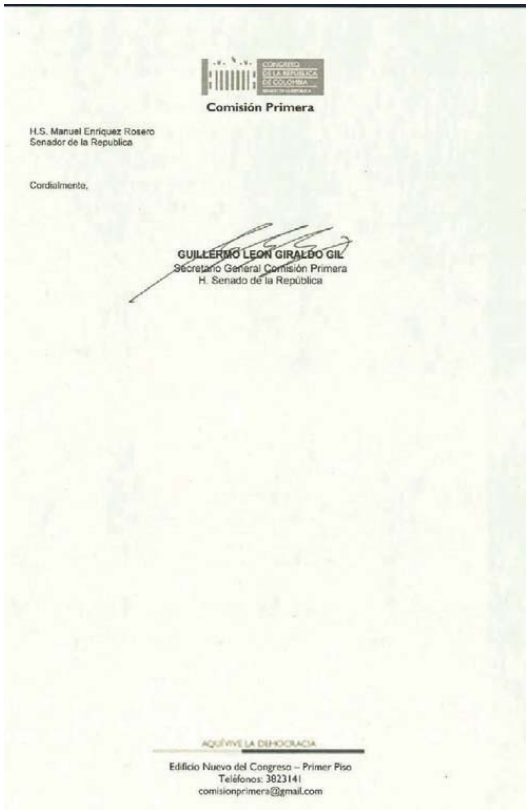
H.S. Doris Clemencia Vega Quiroz
Senadora de la Republica

H.S. Hernán Andrade Serrano
Senador de la Republica

H.S. José Obdulio Gaviria Vélez
Senador de la Republica

AQUÍ VIVE LA DEMOCRACIA

Edificio Nuevo del Congreso – Primer Piso
Teléfonos: 3823141
comisionprimera@gmail.com



Comisión Primera

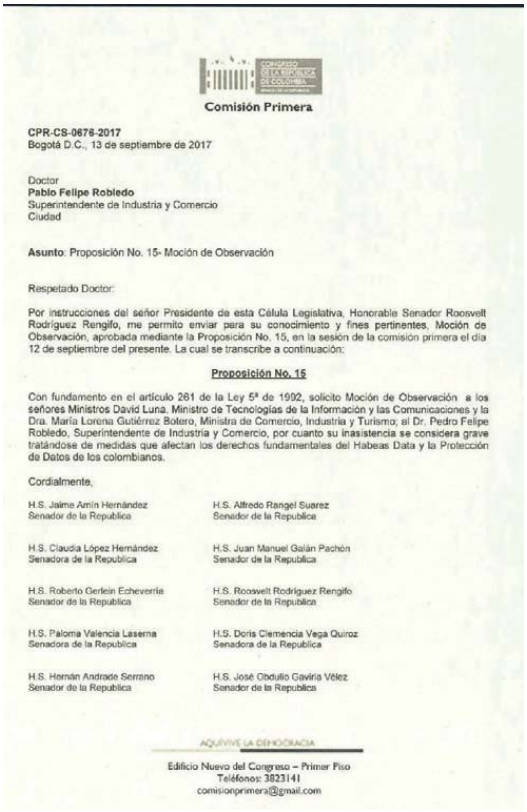
H.S. Manuel Enriquez Rosero
Senador de la Republica

Cordialmente,

GUILLERMO LEON GIRALDO GIL
Secretario General Comisión Primera
H. Senado de la República

AQUÍ VIVE LA DEMOCRACIA

Edificio Nuevo del Congreso – Primer Piso
Teléfonos: 3823141
comisionprimera@gmail.com



Comisión Primera

CPR-CS-0676-2017
Bogotá D.C., 13 de septiembre de 2017

Doctor
Pablo Felipe Robledo
Superintendente de Industria y Comercio
Ciudad

Asunto: Proposición No. 15- Moción de Observación

Respetado Doctor:

Por instrucciones del señor Presidente de esta Célula Legislativa, Honorable Senador Roosvelt Rodríguez Rengifo, me permito enviar para su conocimiento y fines pertinentes, Moción de Observación, aprobada mediante la Proposición No. 15, en la sesión de la comisión primera el día 12 de septiembre del presente. La cual se transcribe a continuación:

Proposición No. 15

Con fundamento en el artículo 261 de la Ley 5ª de 1992, solicito Moción de Observación a los señores Ministros David Luna. Ministro de Tecnologías de la Información y las Comunicaciones y la Dra. María Lorena Gutiérrez Botero, Ministra de Comercio, Industria y Turismo; al Dr. Pedro Felipe Robledo, Superintendente de Industria y Comercio, por cuanto su inasistencia se considera grave tratándose de medidas que afectan los derechos fundamentales del Habeas Data y la Protección de Datos de los colombianos.

Cordialmente,

H.S. Jaime Amín Hernández
Senador de la Republica

H.S. Alfredo Rangel Suarez
Senador de la Republica

H.S. Claudia López Hernández
Senadora de la Republica

H.S. Juan Manuel Galán Pachón
Senador de la Republica

H.S. Roberto Gerlein Echeverría
Senador de la Republica

H.S. Roosvelt Rodríguez Rengifo
Senador de la Republica

H.S. Paloma Valencia Laserna
Senadora de la Republica

H.S. Doris Clemencia Vega Quiroz
Senadora de la Republica

H.S. Hernán Andrade Serrano
Senador de la Republica

H.S. José Obdulio Gaviria Vélez
Senador de la Republica

AQUÍ VIVE LA DEMOCRACIA

Edificio Nuevo del Congreso – Primer Piso
Teléfonos: 3823141
comisionprimera@gmail.com

Comisión Primera

H.S. Manuel Enriquez Rosero
Senador de la Republica

Cordialmente,

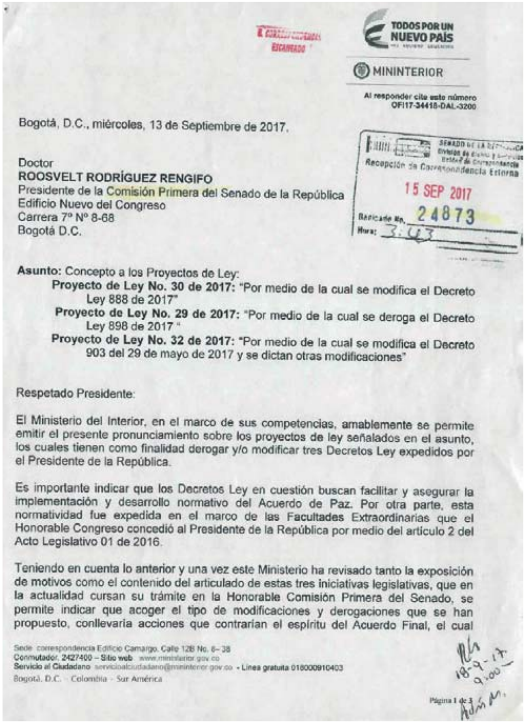
GUILLERMO LEON GIRALDO GIL
Secretario General Comisión Primera
H. Senado de la República

AQUÍ VIVE LA DEMOCRACIA

Edificio Nuevo del Congreso – Primer Piso
Teléfonos: 3823141
comisionprimera@gmail.com

Anexo N° 2

Comentarios a los proyectos de ley: Proyecto de ley número 29 de 2017 Senado, *"por medio de la cual se deroga el Decreto-ley 898 de 2017"*. Proyecto de ley número 30 de 2017 Senado, *"por medio de la cual se modifica el Decreto-ley 888 de 2017"*. Proyecto de ley número 32 de 2017 Senado, *"por medio del cual se modifica el Decreto 903 del 29 de Mayo de 2017 y se dictan otras disposiciones"*. Firmado doctor Guillermo Rivera Flórez – Ministro del Interior.



TODOS POR UN NUEVO PAÍS

MININTERIOR

Al responder cite este número
OFI17-34410-DAL-3200

Bogotá, D.C., miércoles, 13 de Septiembre de 2017.

SENADO DE LA REPÚBLICA
Dirección de Gestión y Servicios
Unidad de Correspondencia
Recepción de Correspondencia Externa
15 SEP 2017
Radicado No. 24873
Hora: 3:03

Doctor
ROOSVELT RODRÍGUEZ RENGIFO
Presidente de la Comisión Primera del Senado de la República
Edificio Nuevo del Congreso
Carrera 7ª Nº 8-68
Bogotá D.C.

Asunto: Concepto a los Proyectos de Ley:

Proyecto de Ley No. 30 de 2017: "Por medio de la cual se modifica el Decreto Ley 888 de 2017"

Proyecto de Ley No. 29 de 2017: "Por medio de la cual se deroga el Decreto Ley 898 de 2017 "

Proyecto de Ley No. 32 de 2017: "Por medio de la cual se modifica el Decreto 903 del 29 de mayo de 2017 y se dictan otras modificaciones"

Respetado Presidente:

El Ministerio del Interior, en el marco de sus competencias, amablemente se permite emitir el presente pronunciamiento sobre los proyectos de ley señalados en el asunto, los cuales tienen como finalidad derogar y/o modificar tres Decretos Ley expedidos por el Presidente de la República.

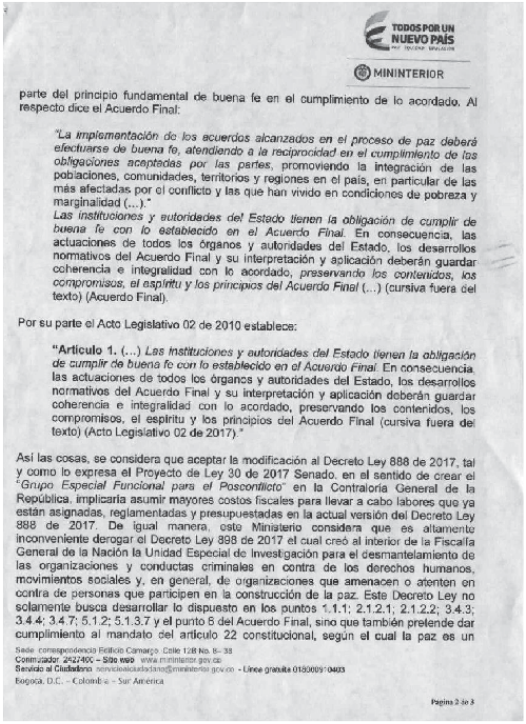
Es importante indicar que los Decretos Ley en cuestión buscan facilitar y asegurar la implementación y desarrollo normativo del Acuerdo de Paz. Por otra parte, esta normatividad fue expedida en el marco de las Facultades Extraordinarias que el Honorable Congreso concedió al Presidente de la República por medio del artículo 2 del Acto Legislativo 01 de 2016.

Teniendo en cuenta lo anterior y una vez este Ministerio ha revisado tanto la exposición de motivos como el contenido del articulado de estas tres iniciativas legislativas, que en la actualidad cursan su trámite en la Honorable Comisión Primera del Senado, se permite indicar que acoger el tipo de modificaciones y derogaciones que se han propuesto, conllevaría acciones que contrarían el espíritu del Acuerdo Final, el cual

18-9-17
9:00

Sede correspondencia Edificio Camargo, Calle 12B No. 8– 38
Conmutador: 2427400 – Sitio web: www.mininterior.gov.co
Servicio al Ciudadano: servicioalciudadano@mininterior.gov.co - Línea gratuita 018000910403
Bogotá, D.C. – Colombia – Sur América

Página 1 de 3



TODOS POR UN NUEVO PAÍS

MININTERIOR

parte del principio fundamental de buena fe en el cumplimiento de lo acordado. Al respecto dice el Acuerdo Final:

> *"La implementación de los acuerdos alcanzados en el proceso de paz deberá efectuarse de buena fe, atendiendo a la reciprocidad en el cumplimiento de las obligaciones aceptadas por las partes*, promoviendo la integración de las poblaciones, comunidades, territorios y regiones en el país, en particular de las más afectadas por el conflicto y las que han vivido en condiciones de pobreza y marginalidad (...)."
> *Las instituciones y autoridades del Estado tienen la obligación de cumplir de buena fe con lo establecido en el Acuerdo Final.* En consecuencia, las actuaciones de todos los órganos y autoridades del Estado, los desarrollos normativos del Acuerdo Final y su interpretación y aplicación deberán guardar coherencia e integralidad con lo acordado, *preservando los contenidos, los compromisos, el espíritu y los principios del Acuerdo Final* (...) (cursiva fuera del texto) (Acuerdo Final).

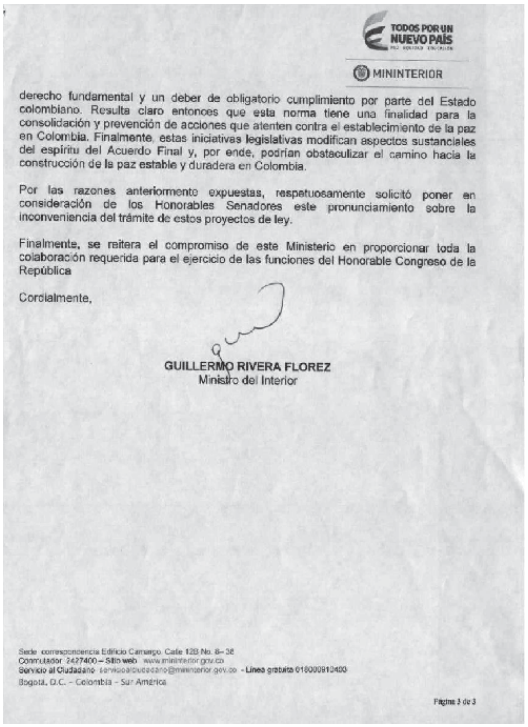
Por su parte el Acto Legislativo 02 de 2010 establece:

> **"Artículo 1.** (...) *Las instituciones y autoridades del Estado tienen la obligación de cumplir de buena fe con lo establecido en el Acuerdo Final.* En consecuencia, las actuaciones de todos los órganos y autoridades del Estado, los desarrollos normativos del Acuerdo Final y su interpretación y aplicación deberán guardar coherencia e integralidad con lo acordado, preservando los contenidos, los compromisos, el espíritu y los principios del Acuerdo Final (cursiva fuera del texto) (Acto Legislativo 02 de 2017)."

Así las cosas, se considera que aceptar la modificación al Decreto Ley 888 de 2017, tal y como lo expresa el Proyecto de Ley 30 de 2017 Senado, en el sentido de crear el *"Grupo Especial Funcional para el Posconflicto"* en la Contraloría General de la República, implicaría asumir mayores costos fiscales para llevar a cabo labores que ya están asignadas, reglamentadas y presupuestadas en la actual versión del Decreto Ley 888 de 2017. De igual manera, este Ministerio considera que es altamente inconveniente derogar el Decreto Ley 898 de 2017 el cual creó al interior de la Fiscalía General de la Nación la Unidad Especial de Investigación para el desmantelamiento de las organizaciones y conductas criminales en contra de los derechos humanos, movimientos sociales y, en general, de organizaciones que amenacen o atenten en contra de personas que participen en la construcción de la paz. Este Decreto Ley no solamente busca desarrollar lo dispuesto en los puntos 1.1.1; 2.1.2.1; 2.1.2.2; 3.4.3; 3.4.4; 3.4.7; 5.1.2; 5.1.3.7 y el punto 6 del Acuerdo Final, sino que también pretende dar cumplimiento al mandato del artículo 22 constitucional, según el cual la paz es un

Sede correspondencia Edificio Camargo, Calle 12B No. 8– 38
Conmutador: 2427400 – Sitio web: www.mininterior.gov.co
Servicio al Ciudadano: servicioalciudadano@mininterior.gov.co - Línea gratuita 018000910403
Bogotá, D.C. – Colombia – Sur América

Página 2 de 3



TODOS POR UN NUEVO PAÍS

MININTERIOR

derecho fundamental y un deber de obligatorio cumplimiento por parte del Estado colombiano. Resulta claro entonces que esta norma tiene una finalidad para la consolidación y prevención de acciones que atenten contra el establecimiento de la paz en Colombia. Finalmente, estas iniciativas legislativas modifican aspectos sustanciales del espíritu del Acuerdo Final y, por ende, podrían obstaculizar el camino hacia la construcción de la paz estable y duradera en Colombia.

Por las razones anteriormente expuestas, respetuosamente solicitó poner en consideración de los Honorables Senadores este pronunciamiento sobre la inconveniencia del trámite de estos proyectos de ley.

Finalmente, se reitera el compromiso de este Ministerio en proporcionar toda la colaboración requerida para el ejercicio de las funciones del Honorable Congreso de la República

Cordialmente,

GUILLERMO RIVERA FLOREZ
Ministro del Interior

Sede correspondencia Edificio Camargo, Calle 12B No. 8– 38
Conmutador: 2427400 – Sitio web: www.mininterior.gov.co
Servicio al Ciudadano: servicioalciudadano@mininterior.gov.co - Línea gratuita 018000910400
Bogotá, D.C. – Colombia – Sur América

Página 3 de 3

Anexo N° 3

Comentarios al Proyecto de ley número 52 de 2017 Senado, *"por medio de la cual se establecen medidas para combatir la corrupción con los recursos públicos destinados a la financiación del sistema general de seguridad social en salud y se dictan otras disposiciones"*. Firmado doctora Marcela Abadía Cubillos Directora de Política Criminal y Penitenciaria - MinJusticia.

MINJUSTICIA TODOS POR UN NUEVO PAÍS

Al responder cite este número
OFI17-0030848-DCP-3200

Bogotá D.C., jueves, 14 de Septiembre de 2017

Recepción de Comisiones/Sesión Externa
14 SEP 2017
Radicado No. 24704
Hora: 3:36

Doctor
GUILLERMO LEÓN GIRALDO GIL
Secretario
Primera Comisión
Senado - Congreso de la República
Carrera 7 – No. 8 - 68
Ciudad

Asunto: Remisión Concepto CSPC, PL 055 de 2017 Senado

Respetado Doctor Giraldo,

De manera atenta, me permito remitirle el concepto emitido por parte del Consejo Superior de Política Criminal al Proyecto de Ley No. 052 de 2017 Senado, "por medio de la cual se establecen medidas para combatir la corrupción con los recursos públicos destinados a la Financiación del Sistema General de Seguridad Social en Salud y se dictan otras disposiciones".

De igual manera, agradezco circular el respectivo concepto a los autores, ponentes y congresistas integrantes de la célula legislativa para su conocimiento y fines pertinentes.

Cordialmente,

MARCELA ABADÍA CUBILLOS
Directora de Política Criminal y Penitenciaria

Anexos: CSPC. Concepto 20.2017. (con (3) folios

Elaboró: Nadia Lizarazo
Aprobó: Marcela Abadía

14-9-17
9:05

Bogotá D.C., Colombia
Calle 53 No. 13 - 27 • Teléfono (57) (1) 444 3100 • www.minjusticia.gov.co

Consejo Superior de Política Criminal MINJUSTICIA TODOS POR UN NUEVO PAÍS

CONSEJO SUPERIOR DE POLÍTICA CRIMINAL

Estudio del Consejo Superior de Política Criminal al Proyecto de Ley No. 052 de 2017 Senado, "por medio de la cual se establecen medidas para combatir la corrupción con los recursos públicos destinados a la Financiación del Sistema General de Seguridad Social en Salud y se dictan otras disposiciones".

Proyecto	No. 052 de 2017 Senado
Título	"Por medio de la cual se establecen medidas para combatir la corrupción con los recursos públicos destinados a la Financiación del Sistema General de Seguridad Social en Salud y se dictan otras disposiciones".
Autor	Senador Fernando Nicolás Araujo y Representante Samuel Alejandro Hoyos.
Fecha de Presentación	27 de julio de 2017
Estado Actual	Espera de designación de ponente
Referencia	Concepto 20.2017

1

El 16 de agosto de 2017 en sesión ordinaria del Comité Técnico del Consejo Superior de Política Criminal se sometió a estudio el Proyecto de Ley No. 052 de 2017 Senado "por medio de la cual se establecen medidas para combatir la corrupción con los recursos públicos destinados a la financiación del Sistema General de Seguridad Social en Salud y se dictan otras disposiciones"

El presente concepto, el cual contiene las consideraciones derivadas del mencionado examen, y se divide en tres apartados. El primero, hace una descripción de la iniciativa legislativa bajo comento. El segundo, contiene una serie de observaciones político-criminales frente a la iniciativa, y por último, se presentan las conclusiones.

1. **Contenido y motivación del Proyecto de Ley No. 052 de 2017 "Por medio de la cual se establecen medidas para combatir la corrupción con los recursos públicos destinados a la Financiación del Sistema General de Seguridad Social en Salud y se dictan otras disposiciones".**

La iniciativa legislativa bajo examen está conformada por cinco (5) artículos incluyendo el de su vigencia y derogatoria.

De acuerdo con el articulado y la exposición motivos, el objeto central de la propuesta normativa es establecer un agravante para la responsabilidad derivada

Bogotá D.C., Colombia
Calle 53 No. 13 - 27 • Teléfono (57) (1) 444 3100 • www.minjusticia.gov.co

Consejo Superior de Política Criminal MINJUSTICIA TODOS POR UN NUEVO PAÍS

de la comisión de tipos penales que tutelan el bien jurídico Administración Pública, en particular aquellas que versan sobre administración y ejecución ilícita de los recursos del erario público destinados a la financiación del Sistema General de Seguridad Social en Salud.

El artículo 2º del Proyecto de Ley propone aumentar el término de prescripción de la acción penal cuando se trate de delitos relacionados con recursos públicos destinados a la financiación del Sistema de General de Seguridad Social en Salud.

Por su parte, el artículo 3º busca modificar el Artículo 399-A de la Ley 599 de 2000 aumentando la pena prevista para el delito de peculado por aplicación oficial diferente frente a recursos de la seguridad social.

Finalmente, el artículo 4º pretende introducir al ordenamiento jurídico penal un nuevo artículo 434-B mediante el cual se crea una circunstancia común de agravación punitiva cuando las conductas punibles recaigan sobre recursos destinados a la financiación del Sistema General de Seguridad Social en Salud.

2. **Consideraciones y observaciones político-criminales al Proyecto de Ley 052 de 2017 "Por medio de la cual se establecen medidas para combatir la corrupción con los recursos públicos destinados a la Financiación del Sistema General de Seguridad Social en Salud y se dictan otras disposiciones".**

2

Luego de la evaluación y discusión del proyecto de ley objeto de estudio y de los argumentos que lo sustentan, el Consejo Superior de Política Criminal conceptúa de manera desfavorable frente a este, con base en las siguientes consideraciones

2.1. La Exposición de Motivos

Como se ha señalado en diversas ocasiones por parte del Consejo Superior de Política Criminal, la lucha contra la corrupción es uno de los temas que deben gozar de especial atención en la agenda pública, no solo para fortalecer los mecanismos existentes en contra de esta modalidad de criminalidad, sino mediante la creación de nuevas medidas dirigidas a evitar afrentas contra la administración y el patrimonio público. Es por ello que las iniciativas que buscuan materializar estos fines deben estar debidamente fundamentadas en aras de garantizar que sus efectos sean los esperados y no impliquen un derroche innecesario de recursos estatales.

Bajo esta perspectiva, respecto del proyecto de ley que se analiza, el Consejo Superior de política Criminal destaca que, si bien la exposición de motivos hace un esfuerzo por caracteriza la corrupción en el sistema de salud, no hace lo mismo en relación con el aumento del término de prescripción de la acción penal y la introducción de una agravación específica, así como una común para las conductas

Bogotá D.C., Colombia
Calle 53 No. 13 - 27 • Teléfono (57) (1) 444 3100 • www.minjusticia.gov.co

Consejo Superior de Política Criminal MINJUSTICIA TODOS POR UN NUEVO PAÍS

que recaen sobre los recursos públicos destinados a la Financiación del Sistema General de Seguridad Social en Salud; así, no se encuentran fundamentos político-criminales concretos que se ocupen de sustentar las reformas propuestas.

La principal observación es que la iniciativa legislativa en su exposición de motivos no sustenta cómo las medidas propuestas *combaten* efectivamente los actos de corrupción relacionados con los recursos destinados al Sistema de Seguridad Social, al tiempo que no demuestra empíricamente los niveles de corrupción en este Sistema, ni tampoco evalúa el impacto de las medidas propuestas.

2.2. Del aumento al término de prescripción de la acción penal

El articulado del Proyecto de Ley analizado propone en su Artículo 2º adicionar un inciso al Artículo 83º de la Ley 599 de 2000, el cual versa sobre el término de prescripción de la acción penal. Establece la reforma en mención que, cuando se trate de delitos que tengan impacto sobre recursos públicos destinados para la financiación del Sistema General de Seguridad Social en Salud, el término de prescripción se aumentará en dos terceras partes.

Recordemos que la prescripción de la acción penal es un derecho que le asiste al individuo en su calidad de procesado cuando, por el trascurso de un determinado lapso de tiempo, no se ha realizado determinada actuación procesal, por lo cual el Estado pierde la facultad de ejercer el *ius puniendi* y *ius persequendi* por las conductas penalmente reprochables que aquel ha perpetrado.

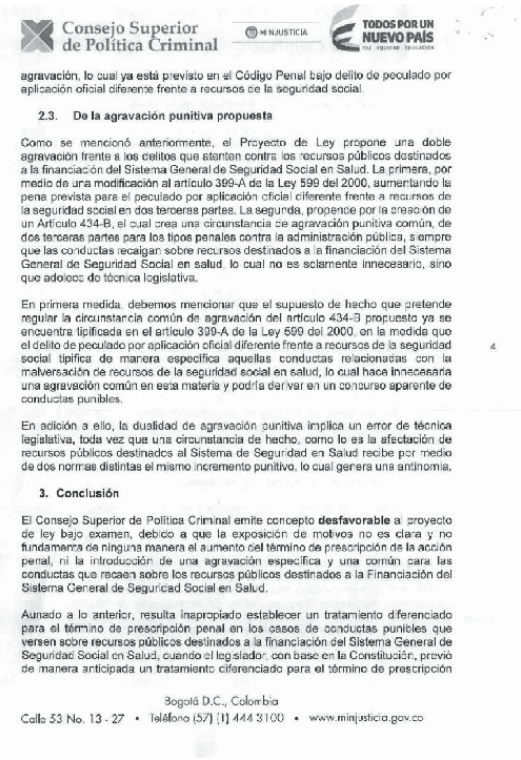
3

El Legislador con base en Artículo 6º de la Constitución, el cual reza que los servidores públicos o quienes ejercen sus funciones de carácter transitorio, no solo responden por infringir la Constitución y las Leyes, sino también por omisión o extralimitación en el ejercicio de sus funciones, previó en el Código Penal un término de prescripción diferenciado atendiendo a la distinción Constitucional de los sujetos, siendo el de los últimos más extenso por su calidad especial.

Dicho lo anterior, no encuentra este órgano colegiado argumento alguno que fundamente la necesidad o la conveniencia de prolongar el término de prescripción de la acción penal en los casos en los cuales las conductas punibles versen sobre recursos públicos destinados para la financiación del Sistema General de Seguridad Social en Salud, toda vez que el legislador ya tuvo en cuenta una diferenciación entre término de prescripción para servidores públicos y particulares; cualquier modificación al respecto debe atender a la un calidad del sujeto activo y no a una circunstancia fáctica como lo es una destinación específica de los recursos públicos.

En adición a ello, la circunstancia de hecho relacionada con la malversación recursos públicos destinados a la Financiación del Sistema General de Seguridad Social implicaría la creación de un tipo penal distinto o una circunstancia de

Bogotá D.C., Colombia
Calle 53 No. 13 - 27 • Teléfono (57) (1) 444 3100 • www.minjusticia.gov.co



Consejo Superior de Política Criminal · MINJUSTICIA · TODOS POR UN NUEVO PAÍS

agravación, lo cual ya está previsto en el Código Penal bajo delito de peculado por aplicación oficial diferente frente a recursos de la seguridad social.

2.3. De la agravación punitiva propuesta

Como se mencionó anteriormente, el Proyecto de Ley propone una doble agravación frente a los delitos que atenten contra los recursos públicos destinados a la financiación del Sistema General de Seguridad Social en Salud. La primera, por medio de una modificación al artículo 399-A de la Ley 599 del 2000, aumentando la pena prevista para el peculado por aplicación oficial diferente frente a recursos de la seguridad social en dos terceras partes. La segunda, propende por la creación de un Artículo 434-B, el cual crea una circunstancia de agravación punitiva común, de dos terceras partes para los tipos penales contra la administración pública, siempre que las conductas recaigan sobre recursos destinados a la financiación del Sistema General de Seguridad Social en salud, lo cual no es sclarnente innecesario, sino que adolece de técnica legislativa.

En primera medida, debemos mencionar que el supuesto de hecho que pretende regular la circunstancia común de agravación del artículo 434-B propuesto ya se encuentra tipificada en el artículo 399-A de la Ley 599 del 2000, en la medida que el delito de peculado por aplicación oficial diferente frente a recursos de la seguridad social tipifica de manera especifica aquellas conductas relacionadas con la malversación de recursos de la seguridad social en salud, lo cual hace innecesaria una agravación común en esta materia y podría derivar en un concurso aparente de conductas punibles.

En adición a ello, la dualidad de agravación punitiva implica un error de técnica legislativa, toda vez que una circunstancia de hecho, como lo es la afectación de recursos públicos destinados al Sistema de Seguridad en Salud recibe por medio de dos normas distintas el mismo incremento punitivo, lo cual genera una antinomia.

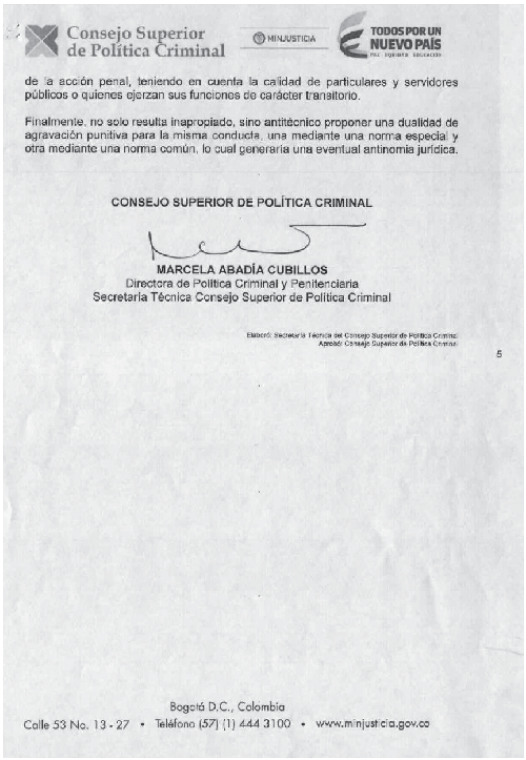
3. Conclusión

El Consejo Superior de Política Criminal emite concepto **desfavorable** al proyecto de ley bajo examen, debido a que la exposición de motivos no es clara y no fundamenta de ninguna manera el aumento del término de prescripción de la acción penal, ni la introducción de una agravación especifica y una común para las conductas que recaen sobre los recursos públicos destinados a la Financiación del Sistema General de Seguridad Social en Salud.

Aunado a lo anterior, resulta inapropiado establecer un tratamiento diferenciado para el término de prescripción penal en los casos de conductas punibles que versen sobre recursos públicos destinados a la financiación del Sistema General de Seguridad Social en Salud, cuando el legislador, con base en la Constitución, previó de manera anticipada un tratamiento diferenciado para el término de prescripción

Bogotá D.C., Colombia
Calle 53 No. 13 - 27 • Teléfono (57) (1) 444 3100 • www.minjusticia.gov.co

4



Consejo Superior de Política Criminal · MINJUSTICIA · TODOS POR UN NUEVO PAÍS

de la acción penal, teniendo en cuenta la calidad de particulares y servidores públicos o quienes ejerzan sus funciones de carácter transitorio.

Finalmente, no solo resulta inapropiado, sino antitécnico proponer una dualidad de agravación punitiva para la misma conducta, una mediante una norma especial y otra mediante una norma común, lo cual generaría una eventual antinomia jurídica.

CONSEJO SUPERIOR DE POLÍTICA CRIMINAL

MARCELA ABADÍA CUBILLOS
Directora de Política Criminal y Penitenciaria
Secretaría Técnica Consejo Superior de Política Criminal

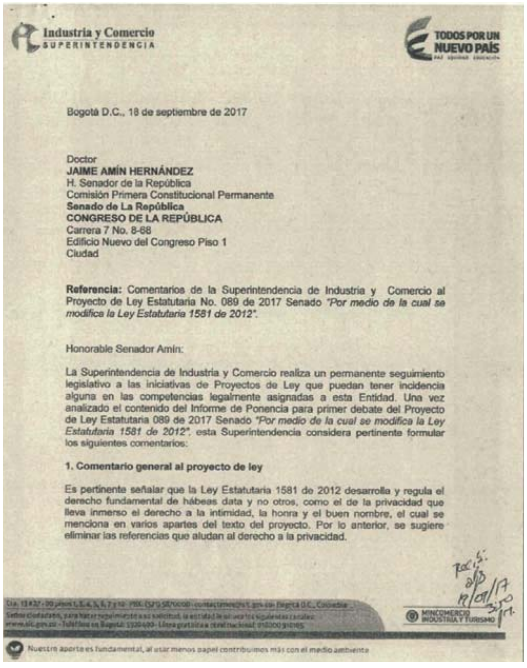
Elaboró: Secretaría Técnica del Consejo Superior de Política Criminal
Aprobó: Consejo Superior de Política Criminal

5

Bogotá D.C., Colombia
Calle 53 No. 13 - 27 • Teléfono (57) (1) 444 3100 • www.minjusticia.gov.co

Anexo N° 4

Comentarios al Proyecto de Ley Estatutaria número 89 de 2017 Senado, *"por medio de la cual se modifica la Ley Estatutaria 1581 de 2012"*. Firmado doctora María Claudia Caviedes Mejía – Superintendencia Delegada para la Protección de los Datos Personales.



Industria y Comercio · SUPERINTENDENCIA · TODOS POR UN NUEVO PAÍS

Bogotá D.C., 18 de septiembre de 2017

Doctor
JAIME AMÍN HERNÁNDEZ
H. Senador de la República
Comisión Primera Constitucional Permanente
Senado de La República
CONGRESO DE LA REPÚBLICA
Carrera 7 No. 8-68
Edificio Nuevo del Congreso Piso 1
Ciudad

Referencia: Comentarios de la Superintendencia de Industria y Comercio al Proyecto de Ley Estatutaria No. 089 de 2017 Senado *"Por medio de la cual se modifica la Ley Estatutaria 1581 de 2012"*.

Honorable Senador Amín:

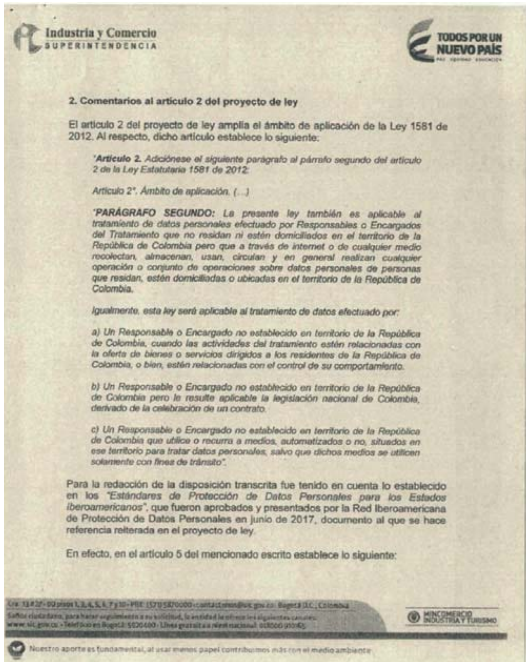
La Superintendencia de Industria y Comercio realiza un permanente seguimiento legislativo a las iniciativas de Proyectos de Ley que puedan tener incidencia alguna en las competencias legalmente asignadas a esta Entidad. Una vez analizado el contenido del Informe de Ponencia para primer debate del Proyecto de Ley Estatutaria 089 de 2017 Senado *"Por medio de la cual se modifica la Ley Estatutaria 1581 de 2012"*, esta Superintendencia considera pertinente formular los siguientes comentarios:

1. Comentario general al proyecto de ley

Es pertinente señalar que la Ley Estatutaria 1581 de 2012 desarrolla y regula el derecho fundamental de hábeas data y no otros, como el de la privacidad que lleva inmerso el derecho a la intimidad, la honra y el buen nombre, el cual se menciona en varios apartes del texto del proyecto. Por lo anterior, se sugiere eliminar las referencias que aludan al derecho a la privacidad.

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

2. Comentarios al artículo 2 del proyecto de ley

El artículo 2 del proyecto de ley amplía el ámbito de aplicación de la Ley 1581 de 2012. Al respecto, dicho artículo establece lo siguiente:

*"**Artículo 2.** Adiciónese el siguiente parágrafo al párrafo segundo del artículo 2 de la Ley Estatutaria 1581 de 2012:*

Artículo 2°. Ámbito de aplicación. (...)

*"**PARÁGRAFO SEGUNDO:** La presente ley también es aplicable al tratamiento de datos personales efectuado por Responsables o Encargados del Tratamiento que no residan ni estén domiciliados en el territorio de la República de Colombia pero que a través de internet o de cualquier medio recolectan, almacenan, usan, circulan y en general realizan cualquier operación o conjunto de operaciones sobre datos personales de personas que residan, estén domiciliadas o ubicadas en el territorio de la República de Colombia.*

Igualmente, esta ley será aplicable al tratamiento de datos efectuado por:

a) Un Responsable o Encargado no establecido en territorio de la República de Colombia, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de la República de Colombia, o bien, estén relacionadas con el control de su comportamiento.

b) Un Responsable o Encargado no establecido en territorio de la República de Colombia pero le resulte aplicable la legislación nacional de Colombia, derivado de la celebración de un contrato.

c) Un Responsable o Encargado no establecido en territorio de la República de Colombia que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito".

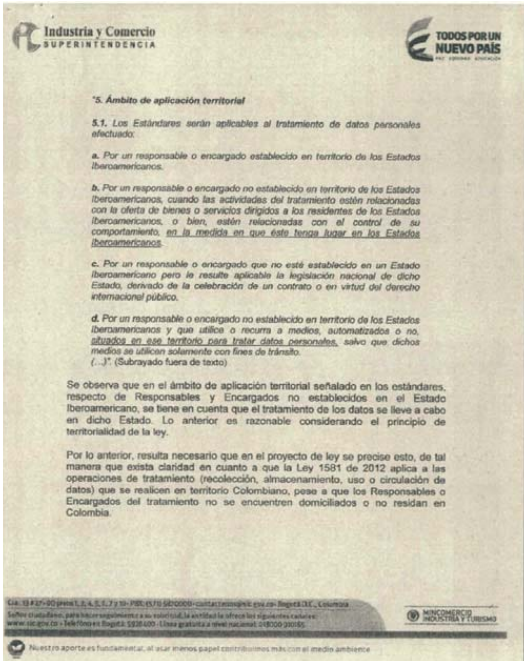
Para la redacción de la disposición transcrita fue tenido en cuenta lo establecido en los *"Estándares de Protección de Datos Personales para los Estados Iberoamericanos"*, que fueron aprobados y presentados por la Red Iberoamericana de Protección de Datos Personales en junio de 2017, documento al que se hace referencia reiterada en el proyecto de ley.

En efecto, en el artículo 5 del mencionado escrito establece lo siguiente:

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

*"**5. Ámbito de aplicación territorial***

***5.1.** Los Estándares serán aplicables al tratamiento de datos personales efectuado:*

***a.** Por un responsable o encargado establecido en territorio de los Estados Iberoamericanos.*

***b.** Por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados Iberoamericanos, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en los Estados Iberoamericanos.*

***c.** Por un responsable o encargado que no esté establecido en un Estado Iberoamericano pero le resulte aplicable la legislación nacional de dicho Estado, derivado de la celebración de un contrato o en virtud del derecho internacional público.*

***d.** Por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito.*
(...)". (Subrayado fuera de texto)

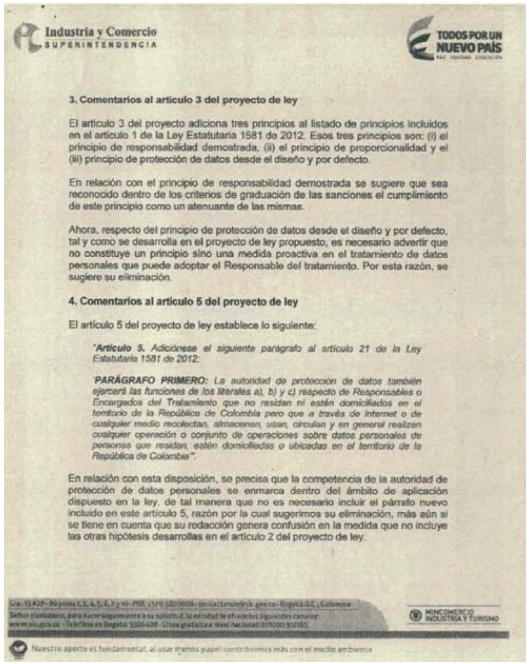
Se observa que en el ámbito de aplicación territorial señalado en los estándares, respecto de Responsables y Encargados no establecidos en el Estado Iberoamericano, se tiene en cuenta que el tratamiento de los datos se lleve a cabo en dicho Estado. Lo anterior es razonable considerando el principio de territorialidad de la ley.

Por lo anterior, resulta necesario que en el proyecto de ley se precise esto, de tal manera que exista claridad en cuanto a que la Ley 1581 de 2012 aplica a las operaciones de tratamiento (recolección, almacenamiento, uso o circulación de datos) que se realicen en territorio Colombiano, pese a que los Responsables o Encargados del tratamiento no se encuentren domiciliados o no residan en Colombia.

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

3. Comentarios al artículo 3 del proyecto de ley

El artículo 3 del proyecto adiciona tres principios al listado de principios incluidos en el artículo 1 de la Ley Estatutaria 1581 de 2012. Esos tres principios son: (i) el principio de responsabilidad demostrada, (ii) el principio de proporcionalidad y el (iii) principio de protección de datos desde el diseño y por defecto.

En relación con el principio de responsabilidad demostrada se sugiere que sea reconocido dentro de los criterios de graduación de las sanciones el cumplimiento de este principio como un atenuante de las mismas.

Ahora, respecto del principio de protección de datos desde el diseño y por defecto, tal y como se desarrolla en el proyecto de ley propuesto, es necesario advertir que no constituye un principio sino una medida proactiva en el tratamiento de datos personales que puede adoptar el Responsable del tratamiento. Por esta razón, se sugiere su eliminación.

4. Comentarios al artículo 5 del proyecto de ley

El artículo 5 del proyecto de ley establece lo siguiente:

*"**Artículo 5.** Adiciónese el siguiente parágrafo al artículo 21 de la Ley Estatutaria 1581 de 2012:*

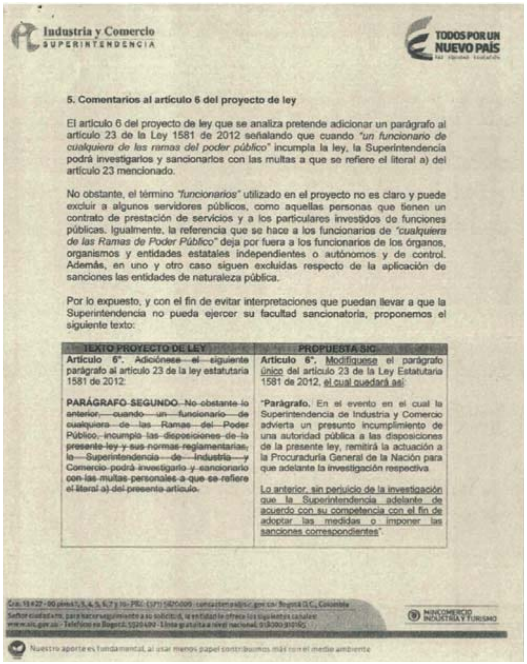
*"**PARÁGRAFO PRIMERO:** La autoridad de protección de datos también ejercerá las funciones de los literales a), b) y c) respecto de Responsables o Encargados del Tratamiento que no residan ni estén domiciliados en el territorio de la República de Colombia pero que a través de internet o de cualquier medio recolectan, almacenan, usan, circulan y en general realizan cualquier operación o conjunto de operaciones sobre datos personales de personas que residan, estén domiciliadas o ubicadas en el territorio de la República de Colombia".*

En relación con esta disposición, se precisa que la competencia de la autoridad de protección de datos personales se enmarca dentro del ámbito de aplicación dispuesto en la ley, de tal manera que no es necesario incluir el párrafo nuevo incluido en este artículo 5, razón por la cual sugerimos su eliminación, más aún si se tiene en cuenta que su redacción genera confusión en la medida que no incluye las otras hipótesis desarrollas en el artículo 2 del proyecto de ley.

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

5. Comentarios al artículo 6 del proyecto de ley

El artículo 6 del proyecto de ley que se analiza pretende adicionar un parágrafo al artículo 23 de la Ley 1581 de 2012 señalando que cuando *"un funcionario de cualquiera de las ramas del poder público"* incumpla la ley, la Superintendencia podrá investigarlos y sancionarlos con las multas a que se refiere el literal a) del artículo 23 mencionado.

No obstante, el término *"funcionarios"* utilizado en el proyecto no es claro y puede excluir a algunos servidores públicos, como aquellas personas que tienen un contrato de prestación de servicios y a los particulares investidos de funciones públicas. Igualmente, la referencia que se hace a los funcionarios de *"cualquiera de las Ramas de Poder Público"* deja por fuera a los funcionarios de los órganos, organismos y entidades estatales independientes o autónomos y de control. Además, en uno y otro caso siguen excluidas respecto de la aplicación de sanciones las entidades de naturaleza pública.

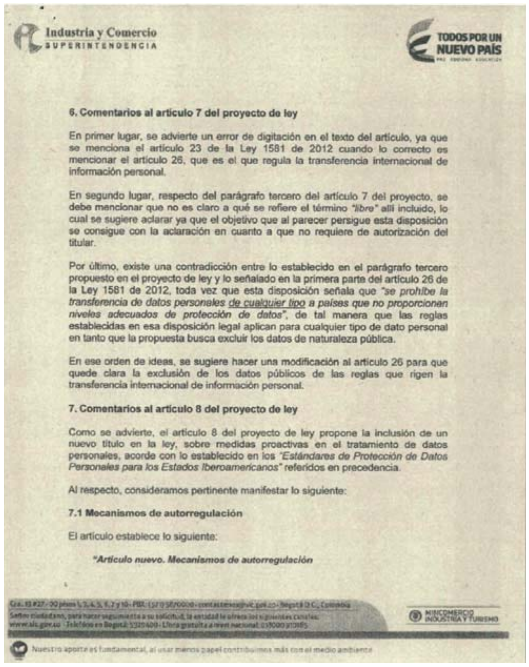
Por lo expuesto, y con el fin de evitar interpretaciones que puedan llevar a que la Superintendencia no pueda ejercer su facultad sancionatoria, proponemos el siguiente texto:

TEXTO PROYECTO DE LEY	PROPUESTA SIC
Artículo 6°. ~~Adiciónese el siguiente~~ parágrafo al artículo 23 de la ley estatutaria 1581 de 2012.	**Artículo 6°.** Modifíquese el parágrafo único del artículo 23 de la Ley Estatutaria 1581 de 2012, el cual quedará así:
~~**PARÁGRAFO SEGUNDO.** No obstante lo anterior, cuando un funcionario de cualquiera de las Ramas del Poder Público, incumpla las disposiciones de la presente ley y sus normas reglamentarias, la Superintendencia de Industria y Comercio podrá investigarlo y sancionarlo con las multas personales a que se refiere el literal a) del presente artículo.~~	**"Parágrafo.** En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva. Lo anterior, sin perjuicio de la investigación que la Superintendencia adelante de acuerdo con su competencia con el fin de adoptar las medidas o imponer las sanciones correspondientes".

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

6. Comentarios al artículo 7 del proyecto de ley

En primer lugar, se advierte un error de digitación en el texto del artículo, ya que se menciona el artículo 23 de la Ley 1581 de 2012 cuando lo correcto es mencionar el artículo 26, que es el que regula la transferencia internacional de información personal.

En segundo lugar, respecto del parágrafo tercero del artículo 7 del proyecto, se debe mencionar que no es claro a qué se refiere el término *"libre"* allí incluido, lo cual se sugiere aclarar ya que el objetivo que al parecer persigue esta disposición se consigue con la aclaración en cuanto a que no requiere de autorización del titular.

Por último, existe una contradicción entre lo establecido en el parágrafo tercero propuesto en el proyecto de ley y lo señalado en la primera parte del artículo 26 de la Ley 1581 de 2012, toda vez que esta disposición señala que *"se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos"*, de tal manera que las reglas establecidas en esa disposición legal aplican para cualquier tipo de dato personal en tanto que la propuesta busca excluir los datos de naturaleza pública.

En ese orden de ideas, se sugiere hacer una modificación al artículo 26 para que quede clara la exclusión de los datos públicos de las reglas que rigen la transferencia internacional de información personal.

7. Comentarios al artículo 8 del proyecto de ley

Como se advierte, el artículo 8 del proyecto de ley propone la inclusión de un nuevo título en la ley, sobre medidas proactivas en el tratamiento de datos personales, acorde con lo establecido en los *"Estándares de Protección de Datos Personales para los Estados Iberoamericanos"* referidos en precedencia.

Al respecto, consideramos pertinente manifestar lo siguiente:

7.1 Mecanismos de autorregulación

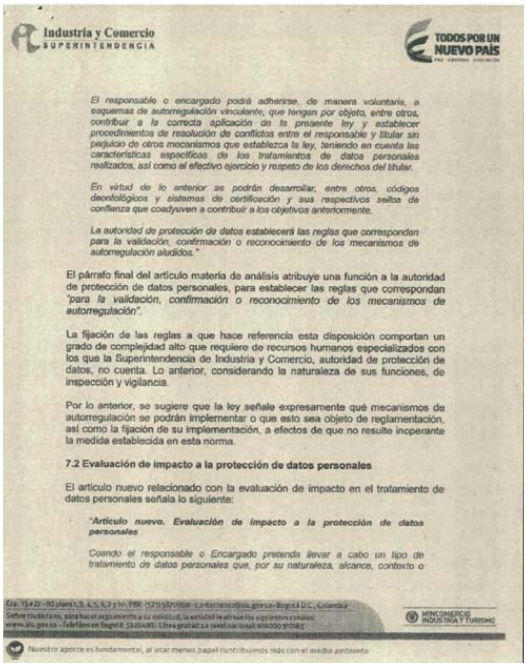
El artículo establece lo siguiente:

"Artículo nuevo. Mecanismos de autorregulación

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (57 1) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfonos en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

El responsable o encargado podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta aplicación de la presente ley y establecer procedimientos de resolución de conflictos entre el responsable y titular sin perjuicio de otros mecanismos que establezca la ley, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del titular.

En virtud de lo anterior se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza que coadyuven a contribuir a los objetivos anteriormente.

La autoridad de protección de datos establecerá las reglas que correspondan para la validación, confirmación o reconocimiento de los mecanismos de autorregulación aludidos."

El párrafo final del artículo materia de análisis atribuye una función a la autoridad de protección de datos personales, para establecer las reglas que correspondan *"para la validación, confirmación o reconocimiento de los mecanismos de autorregulación"*.

La fijación de las reglas a que hace referencia esta disposición comportan un grado de complejidad alto que requiere de recursos humanos especializados con los que la Superintendencia de Industria y Comercio, autoridad de protección de datos, no cuenta. Lo anterior, considerando la naturaleza de sus funciones, de inspección y vigilancia.

Por lo anterior, se sugiere que la ley señale expresamente qué mecanismos de autorregulación se podrán implementar o que esto sea objeto de reglamentación, así como la fijación de su implementación, a efectos de que no resulte inoperante la medida establecida en esta norma.

7.2 Evaluación de impacto a la protección de datos personales

El artículo nuevo relacionado con la evaluación de impacto en el tratamiento de datos personales señala lo siguiente:

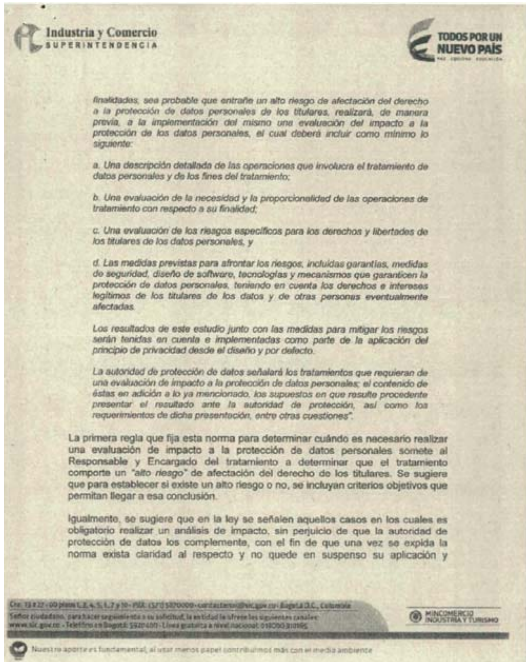
"Artículo nuevo. Evaluación de impacto a la protección de datos personales

Cuando el responsable o Encargado pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (57 1) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfonos en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales, el cual deberá incluir como mínimo lo siguiente:

a. Una descripción detallada de las operaciones que involucra el tratamiento de datos personales y de los fines del tratamiento;

b. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c. Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales, y

d. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas.

Los resultados de este estudio junto con las medidas para mitigar los riesgos serán tenidas en cuenta e implementadas como parte de la aplicación del principio de privacidad desde el diseño y por defecto.

La autoridad de protección de datos señalará los tratamientos que requieran de una evaluación de impacto a la protección de datos personales; el contenido de éstas en adición a lo ya mencionado, los supuestos en que resulte procedente presentar el resultado ante la autoridad de protección, así como los requerimientos de dicha presentación, entre otras cuestiones".

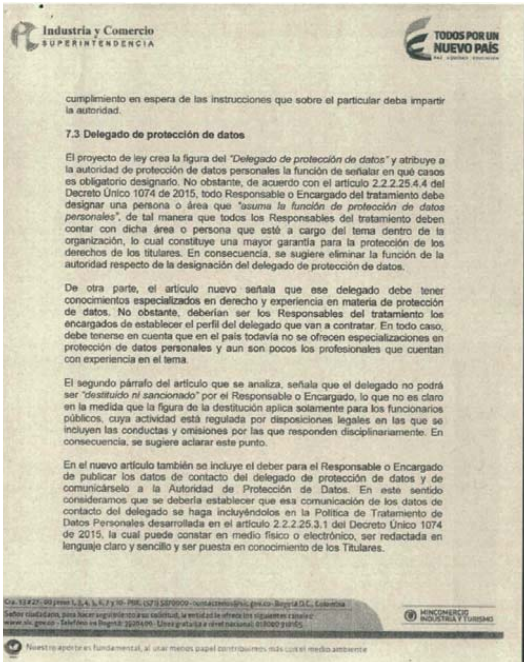
La primera regla que fija esta norma para determinar cuándo es necesario realizar una evaluación de impacto a la protección de datos personales somete al Responsable y Encargado del tratamiento a determinar que el tratamiento comporte un *"alto riesgo"* de afectación del derecho de los titulares. Se sugiere que para establecer si existe un alto riesgo o no, se incluyan criterios objetivos que permitan llegar a esa conclusión.

Igualmente, se sugiere que en la ley se señalen aquellos casos en los cuales es obligatorio realizar un análisis de impacto, sin perjuicio de que la autoridad de protección de datos los complemente, con el fin de que una vez se expida la norma exista claridad al respecto y no quede en suspenso su aplicación y

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (57 1) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfonos en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

cumplimiento en espera de las instrucciones que sobre el particular deba impartir la autoridad.

7.3 Delegado de protección de datos

El proyecto de ley crea la figura del *"Delegado de protección de datos"* y atribuye a la autoridad de protección de datos personales la función de señalar en qué casos es obligatorio designarlo. No obstante, de acuerdo con el artículo 2.2.2.25.4.4 del Decreto Único 1074 de 2015, todo Responsable o Encargado del tratamiento debe designar una persona o área que *"asuma la función de protección de datos personales"*, de tal manera que todos los Responsables del tratamiento deben contar con dicha área o persona que esté a cargo del tema dentro de la organización, lo cual constituye una mayor garantía para la protección de los derechos de los titulares. En consecuencia, se sugiere eliminar la función de la autoridad respecto de la designación del delegado de protección de datos.

De otra parte, el artículo nuevo señala que ese delegado debe tener conocimientos especializados en derecho y experiencia en materia de protección de datos. No obstante, deberían ser los Responsables del tratamiento los encargados de establecer el perfil del delegado que van a contratar. En todo caso, debe tenerse en cuenta que en el país todavía no se ofrecen especializaciones en protección de datos personales y aun son pocos los profesionales que cuentan con experiencia en el tema.

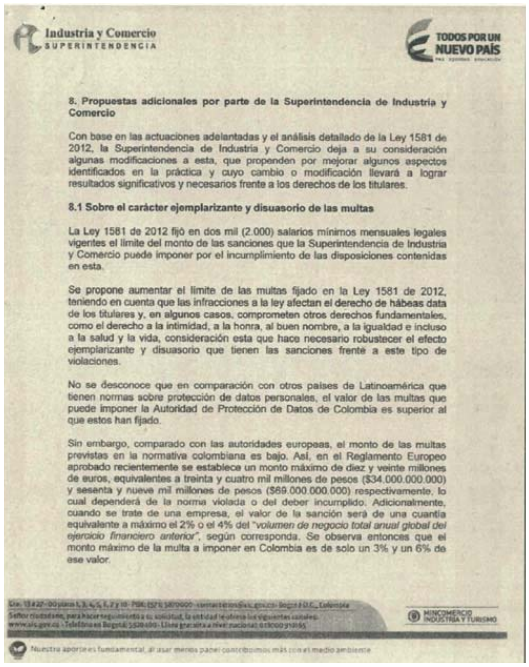
El segundo párrafo del artículo que se analiza, señala que el delegado no podrá ser *"destituido ni sancionado"* por el Responsable o Encargado, lo que no es claro en la medida que la figura de la destitución aplica solamente para los funcionarios públicos, cuya actividad está regulada por disposiciones legales en las que se incluyen las conductas y omisiones por las que responden disciplinariamente. En consecuencia, se sugiere aclarar este punto.

En el nuevo artículo también se incluye el deber para el Responsable o Encargado de publicar los datos de contacto del delegado de protección de datos y de comunicárselo a la Autoridad de Protección de Datos. En este sentido consideramos que se debería establecer que esa comunicación de los datos de contacto del delegado se haga incluyéndolos en la Política de Tratamiento de Datos Personales desarrollada en el artículo 2.2.2.25.3.1 del Decreto Único 1074 de 2015, la cual puede constar en medio físico o electrónico, ser redactada en lenguaje claro y sencillo y ser puesta en conocimiento de los Titulares.

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (57 1) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfonos en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

8. Propuestas adicionales por parte de la Superintendencia de Industria y Comercio

Con base en las actuaciones adelantadas y el análisis detallado de la Ley 1581 de 2012, la Superintendencia de Industria y Comercio deja a su consideración algunas modificaciones a esta, que propenden por mejorar algunos aspectos identificados en la práctica y cuyo cambio o modificación llevará a lograr resultados significativos y necesarios frente a los derechos de los titulares.

8.1 Sobre el carácter ejemplarizante y disuasorio de las multas

La Ley 1581 de 2012 fijó en dos mil (2.000) salarios mínimos mensuales legales vigentes el límite del monto de las sanciones que la Superintendencia de Industria y Comercio puede imponer por el incumplimiento de las disposiciones contenidas en esta.

Se propone aumentar el límite de las multas fijado en la Ley 1581 de 2012, teniendo en cuenta que las infracciones a la ley afectan el derecho de hábeas data de los titulares y, en algunos casos, comprometen otros derechos fundamentales, como el derecho a la intimidad, a la honra, al buen nombre, a la igualdad e incluso a la salud y la vida, consideración esta que hace necesario robustecer el efecto ejemplarizante y disuasorio que tienen las sanciones frente a este tipo de violaciones.

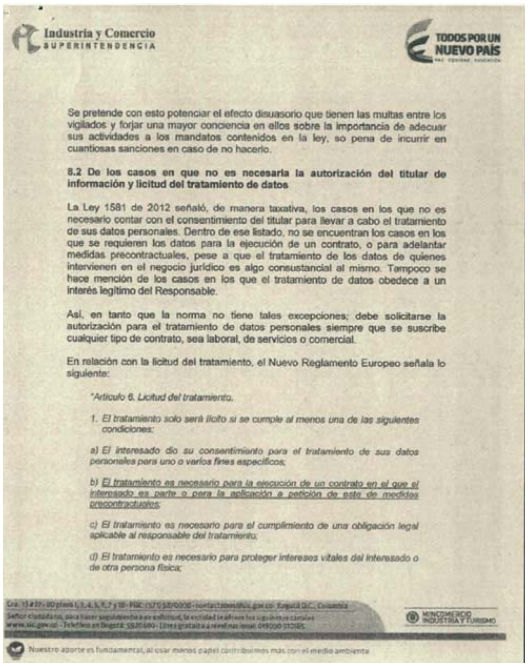
No se desconoce que en comparación con otros países de Latinoamérica que tienen normas sobre protección de datos personales, el valor de las multas que puede imponer la Autoridad de Protección de Datos de Colombia es superior al que estos han fijado.

Sin embargo, comparado con las autoridades europeas, el monto de las multas previstas en la normativa colombiana es bajo. Así, en el Reglamento Europeo aprobado recientemente se establece un monto máximo de diez y veinte millones de euros, equivalentes a treinta y cuatro mil millones de pesos ($34.000.000.000) y sesenta y nueve mil millones de pesos ($69.000.000.000) respectivamente, lo cual dependerá de la norma violada o del deber incumplido. Adicionalmente, cuando se trate de una empresa, el valor de la sanción será de una cuantía equivalente a máximo el 2% o el 4% del "*volumen de negocio total anual global del ejercicio financiero anterior*", según corresponda. Se observa entonces que el monto máximo de la multa a imponer en Colombia es de solo un 3% y un 6% de ese valor.

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (57) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

Se pretende con esto potenciar el efecto disuasorio que tienen las multas entre los vigilados y forjar una mayor conciencia en ellos sobre la importancia de adecuar sus actividades a los mandatos contenidos en la ley, so pena de incurrir en cuantiosas sanciones en caso de no hacerlo.

8.2 De los casos en que no es necesaria la autorización del titular de información y licitud del tratamiento de datos

La Ley 1581 de 2012 señaló, de manera taxativa, los casos en los que no es necesario contar con el consentimiento del titular para llevar a cabo el tratamiento de sus datos personales. Dentro de ese listado, no se encuentran los casos en los que se requieren los datos para la ejecución de un contrato, o para adelantar medidas precontractuales, pese a que el tratamiento de los datos de quienes intervienen en el negocio jurídico es algo consustancial al mismo. Tampoco se hace mención de los casos en los que el tratamiento de datos obedece a un interés legítimo del Responsable.

Así, en tanto que la norma no tiene tales excepciones; debe solicitarse la autorización para el tratamiento de datos personales siempre que se suscribe cualquier tipo de contrato, sea laboral, de servicios o comercial.

En relación con la licitud del tratamiento, el Nuevo Reglamento Europeo señala lo siguiente:

"Artículo 6. Licitud del tratamiento.

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

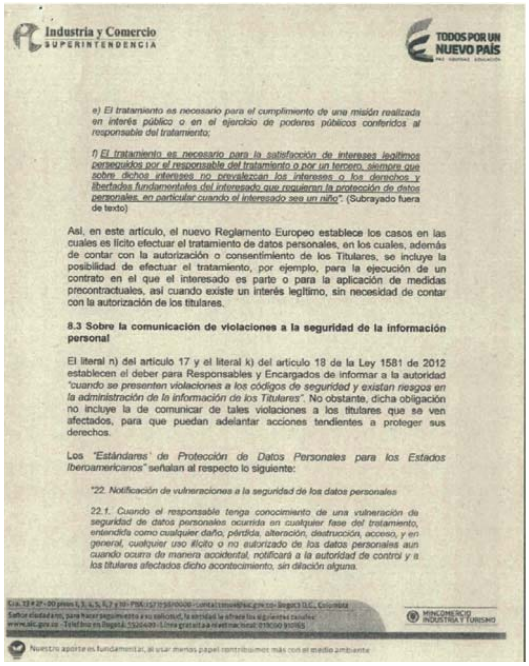
c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (57) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

e) El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño". (Subrayado fuera de texto)

Así, en este artículo, el nuevo Reglamento Europeo establece los casos en las cuales es lícito efectuar el tratamiento de datos personales, en los cuales, además de contar con la autorización o consentimiento de los Titulares, se incluye la posibilidad de efectuar el tratamiento, por ejemplo, para la ejecución de un contrato en el que el interesado es parte o para la aplicación de medidas precontractuales, así cuando existe un interés legítimo, sin necesidad de contar con la autorización de los titulares.

8.3 Sobre la comunicación de violaciones a la seguridad de la información personal

El literal n) del artículo 17 y el literal k) del artículo 18 de la Ley 1581 de 2012 establecen el deber para Responsables y Encargados de informar a la autoridad *"cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares"*. No obstante, dicha obligación no incluye la de comunicar de tales violaciones a los titulares que se ven afectados, para que puedan adelantar acciones tendientes a proteger sus derechos.

Los *"Estándares de Protección de Datos Personales para los Estados Iberoamericanos"* señalan al respecto lo siguiente:

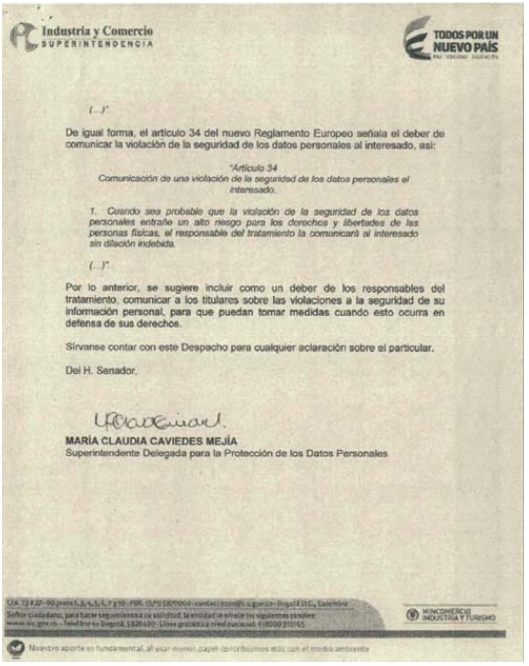
"22. Notificación de vulneraciones a la seguridad de los datos personales

22.1. Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, notificará a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna.

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (57) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

(...)".

De igual forma, el artículo 34 del nuevo Reglamento Europeo señala el deber de comunicar la violación de la seguridad de los datos personales al interesado, así:

"Artículo 34
Comunicación de una violación de la seguridad de los datos personales al interesado.

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

(...)".

Por lo anterior, se sugiere incluir como un deber de los responsables del tratamiento, comunicar a los titulares sobre las violaciones a la seguridad de su información personal, para que puedan tomar medidas cuando esto ocurra en defensa de sus derechos.

Sírvanse contar con este Despacho para cualquier aclaración sobre el particular.

Del H. Senador,

MARÍA CLAUDIA CAVIEDES MEJÍA
Superintendente Delegada para la Protección de los Datos Personales

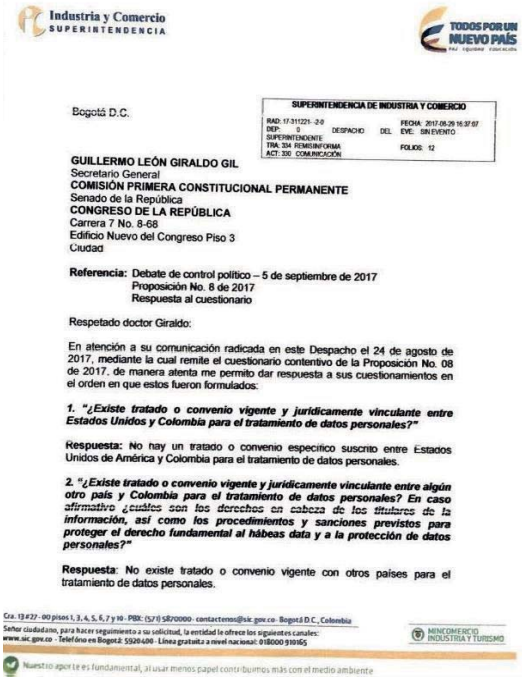
Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (57) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente

Anexo N° 5

Respuesta debate control político Proposición número 8 Superintendencia de Industria y Comercio



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
RAD: 17-311221- 2-0
DEP: 0 DESPACHO DEL FECHA: 2017-08-29 16:37:07
SUPERINTENDENTE EVE: SIN EVENTO
TRA: 334 REMISIÓN/FORMA
ACT: 330 COMUNICACIÓN FOLIOS: 12

Bogotá D.C.

GUILLERMO LEÓN GIRALDO GIL
Secretario General
COMISIÓN PRIMERA CONSTITUCIONAL PERMANENTE
Senado de la República
CONGRESO DE LA REPÚBLICA
Carrera 7 No. 8-68
Edificio Nuevo del Congreso Piso 3
Ciudad

Referencia: Debate de control político – 5 de septiembre de 2017
Proposición No. 8 de 2017
Respuesta al cuestionario

Respetado doctor Giraldo:

En atención a su comunicación radicada en este Despacho el 24 de agosto de 2017, mediante la cual remite el cuestionario contentivo de la Proposición No. 08 de 2017, de manera atenta me permito dar respuesta a sus cuestionamientos en el orden en que estos fueron formulados:

1. "¿Existe tratado o convenio vigente y jurídicamente vinculante entre Estados Unidos y Colombia para el tratamiento de datos personales?"

Respuesta: No hay un tratado o convenio específico suscrito entre Estados Unidos de América y Colombia para el tratamiento de datos personales.

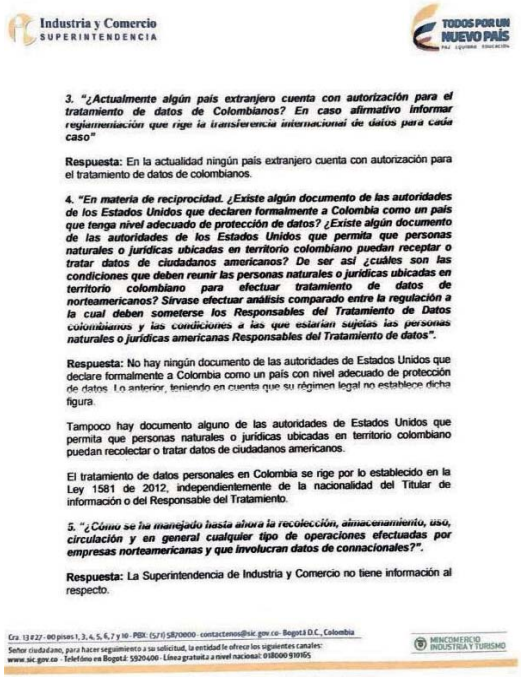
2. "¿Existe tratado o convenio vigente y jurídicamente vinculante entre algún otro país y Colombia para el tratamiento de datos personales? En caso afirmativo ¿cuáles son los derechos en cabeza de los titulares de la información, así como los procedimientos y sanciones previstos para proteger el derecho fundamental al hábeas data y a la protección de datos personales?"

Respuesta: No existe tratado o convenio vigente con otros países para el tratamiento de datos personales.

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

3. "¿Actualmente algún país extranjero cuenta con autorización para el tratamiento de datos de Colombianos? En caso afirmativo informar reglamentación que rige la transferencia internacional de datos para cada caso"

Respuesta: En la actualidad ningún país extranjero cuenta con autorización para el tratamiento de datos de colombianos.

4. "En materia de reciprocidad. ¿Existe algún documento de las autoridades de los Estados Unidos que declaren formalmente a Colombia como un país que tenga nivel adecuado de protección de datos? ¿Existe algún documento de las autoridades de los Estados Unidos que permita que personas naturales o jurídicas ubicadas en territorio colombiano puedan receptar o tratar datos de ciudadanos americanos? De ser así ¿cuáles son las condiciones que deben reunir las personas naturales o jurídicas ubicadas en territorio colombiano para efectuar tratamiento de datos de norteamericanos? Sírvase efectuar análisis comparado entre la regulación a la cual deben someterse los Responsables del Tratamiento de Datos colombianos y las condiciones a las que estarían sujetas las personas naturales o jurídicas americanas Responsables del Tratamiento de datos".

Respuesta: No hay ningún documento de las autoridades de Estados Unidos que declare formalmente a Colombia como un país con nivel adecuado de protección de datos. Lo anterior, teniendo en cuenta que su régimen legal no establece dicha figura.

Tampoco hay documento alguno de las autoridades de Estados Unidos que permita que personas naturales o jurídicas ubicadas en territorio colombiano puedan recolectar o tratar datos de ciudadanos americanos.

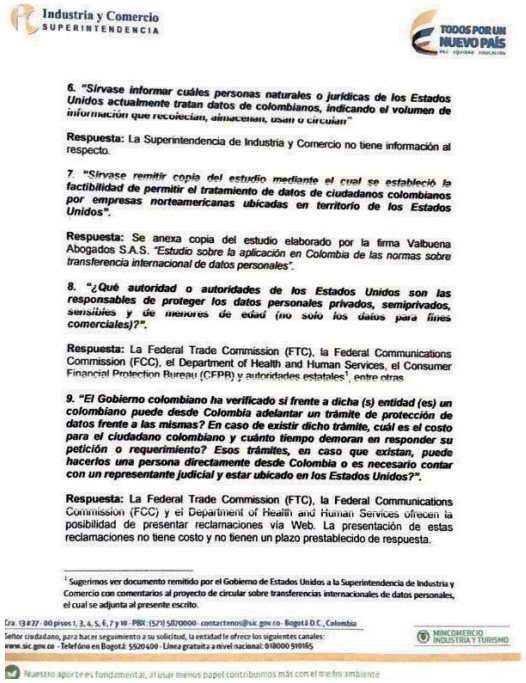
El tratamiento de datos personales en Colombia se rige por lo establecido en la Ley 1581 de 2012, independientemente de la nacionalidad del Titular de información o del Responsable del Tratamiento.

5. "¿Cómo se ha manejado hasta ahora la recolección, almacenamiento, uso, circulación y en general cualquier tipo de operaciones efectuadas por empresas norteamericanas y que involucran datos de connacionales?".

Respuesta: La Superintendencia de Industria y Comercio no tiene información al respecto.

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

6. "Sírvase informar cuáles personas naturales o jurídicas de los Estados Unidos actualmente tratan datos de colombianos, indicando el volumen de información que recolectan, almacenan, usan o circulan"

Respuesta: La Superintendencia de Industria y Comercio no tiene información al respecto.

7. "Sírvase remitir copia del estudio mediante el cual se estableció la factibilidad de permitir el tratamiento de datos de ciudadanos colombianos por empresas norteamericanas ubicadas en territorio de los Estados Unidos".

Respuesta: Se anexa copia del estudio elaborado por la firma Valbuena Abogados S.A.S. *"Estudio sobre la aplicación en Colombia de las normas sobre transferencia internacional de datos personales"*.

8. "¿Qué autoridad o autoridades de los Estados Unidos son las responsables de proteger los datos personales privados, semiprivados, sensibles y de menores de edad (no solo los datos para fines comerciales)?".

Respuesta: La Federal Trade Commission (FTC), la Federal Communications Commission (FCC), el Department of Health and Human Services, el Consumer Financial Protection Bureau (CFPB) y autoridades estatales[1], entre otras.

9. "El Gobierno colombiano ha verificado si frente a dicha (s) entidad (es) un colombiano puede desde Colombia adelantar un trámite de protección de datos frente a las mismas? En caso de existir dicho trámite, cuál es el costo para el ciudadano colombiano y cuánto tiempo demoran en responder su petición o requerimiento? Esos trámites, en caso que existan, puede hacerlos una persona directamente desde Colombia o es necesario contar con un representante judicial y estar ubicado en los Estados Unidos?".

Respuesta: La Federal Trade Commission (FTC), la Federal Communications Commission (FCC) y el Department of Health and Human Services ofrecen la posibilidad de presentar reclamaciones vía Web. La presentación de estas reclamaciones no tiene costo y no tienen un plazo prestablecido de respuesta.

[1] Sugerimos ver documento remitido por el Gobierno de Estados Unidos a la Superintendencia de Industria y Comercio con comentarios al proyecto de circular sobre transferencias internacionales de datos personales, el cual se adjunta al presente escrito.

Cra. 13 #27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Nuestro aporte es fundamental, al usar menos papel contribuimos más con el medio ambiente

Industria y Comercio
SUPERINTENDENCIA

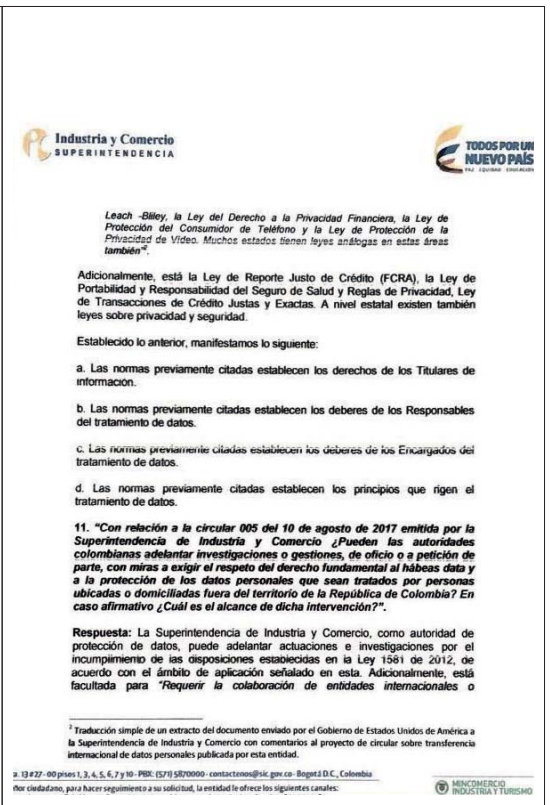
TODOS POR UN NUEVO PAÍS

10. "El artículo 26 de la Ley 1581 de 2012 ordena que los estándares fijados por la Superintendencia de Industria y Comercio sobre nivel adecuado de protección de datos, "en ningún caso podrán ser inferiores" a los que exige la ley 1581 de 2012 a sus destinatarios. Así las cosas, de qué manera el Gobierno Nacional verificó que la regulación e instituciones de los Estados Unidos tiene un nivel igual o superior al que exige la ley 1581 de 2012? En particular, responder lo siguiente: a) En qué normas de los Estados Unidos se hace referencia a todos los derechos que exige el artículo 8 de la ley 1581 de 2012 respecto de todo tipo de dato personal –privado, sensible, semiprivado y de los menores de edad-? En los Estados Unidos se garantizan los mismos derechos que en Colombia?; b) En qué normas de los Estados Unidos se hace referencia a todas las obligaciones que deben cumplir los Responsables del Tratamiento que exige el artículo 17 de la ley 1581 de 2012 respecto de todo tipo de dato personal –privado, sensible, semiprivado y de los menores de edad-? En los Estados Unidos se exigen a los Responsables las mismos obligaciones que en Colombia?; c) En qué normas de los Estados Unidos se hace referencia a todas las obligaciones que deben cumplir los Encargados del Tratamiento que exige el artículo 17 de la ley 1581 de 2012 respecto de todo tipo de dato personal –privado, sensible, semiprivado y de los menores de edad-? En los Estados Unidos se exigen a los Encargados las mismos obligaciones que en Colombia?; d) En qué normas de los Estados Unidos se hace referencia a todos los principios que exige el artículo 4 de la ley 1581 de 2012 respecto del tratamiento de todo tipo de dato personal –privado, sensible, semiprivado y de los menores de edad-? En los Estados Unidos rigen los mismos principios para el tratamiento de datos que exige la ley 1581 de 2012?".

Respuesta: El ordenamiento jurídico de los Estados Unidos de América es diferente al ordenamiento jurídico colombiano en materia de protección de datos personales. El régimen jurídico de privacidad del mencionado país cuenta con varias normas sectoriales que de forma independiente regulan la protección de dicho derecho. Entre otras, dicho régimen se compone de las siguientes disposiciones:

"(...)

Muchas leyes federales regulan la recolección y el uso comercial de información personal, más allá de la Sección 5 de la Ley de la FTC, incluyendo: la Ley de Política de Comunicaciones por Cable, la Ley de Protección de Privacidad en Línea de Niños (COPPA), la Ley de Protección de la Privacidad de los Conductores, la Ley de Privacidad de Comunicaciones Electrónicas. La Ley de Transferencia Electrónica de Fondos, la Ley Gramm-



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

Leach -Bliley, la Ley del Derecho a la Privacidad Financiera, la Ley de Protección del Consumidor de Teléfono y la Ley de Protección de la Privacidad de Video. Muchos estados tienen leyes análogas en estas áreas también"[1].

Adicionalmente, está la Ley de Reporte Justo de Crédito (FCRA), la Ley de Portabilidad y Responsabilidad del Seguro de Salud y Reglas de Privacidad, Ley de Transacciones de Crédito Justas y Exactas. A nivel estatal existen también leyes sobre privacidad y seguridad.

Establecido lo anterior, manifestamos lo siguiente:

a. Las normas previamente citadas establecen los derechos de los Titulares de información.

b. Las normas previamente citadas establecen los deberes de los Responsables del tratamiento de datos.

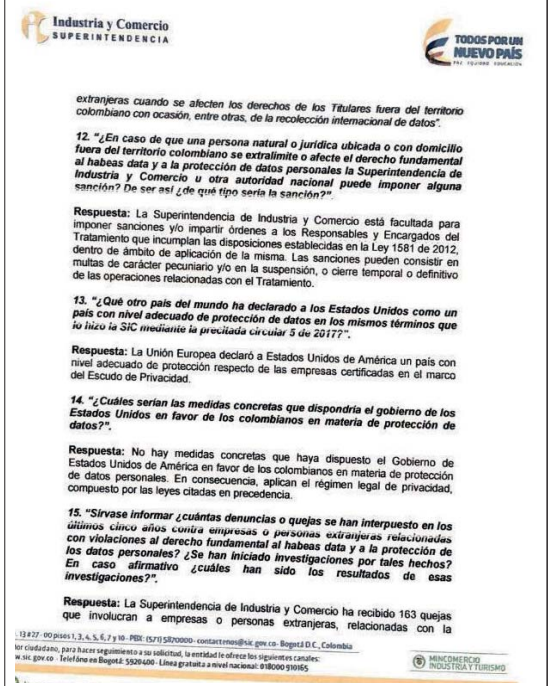
c. Las normas previamente citadas establecen los deberes de los Encargados del tratamiento de datos.

d. Las normas previamente citadas establecen los principios que rigen el tratamiento de datos.

11. *"Con relación a la circular 005 del 10 de agosto de 2017 emitida por la Superintendencia de Industria y Comercio ¿Pueden las autoridades colombianas adelantar investigaciones o gestiones, de oficio o a petición de parte, con miras a exigir el respeto del derecho fundamental al hábeas data y a la protección de los datos personales que sean tratados por personas ubicadas o domiciliadas fuera del territorio de la República de Colombia? En caso afirmativo ¿Cuál es el alcance de dicha intervención?".*

Respuesta: La Superintendencia de Industria y Comercio, como autoridad de protección de datos, puede adelantar actuaciones e investigaciones por el incumplimiento de las disposiciones establecidas en la Ley 1581 de 2012, de acuerdo con el ámbito de aplicación señalado en esta. Adicionalmente, está facultada para *"Requerir la colaboración de entidades internacionales o*

[1] Traducción simple de un extracto del documento enviado por el Gobierno de Estados Unidos de América a la Superintendencia de Industria y Comercio con comentarios al proyecto de circular sobre transferencia internacional de datos personales publicada por esta entidad.



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos".

12. *"¿En caso de que una persona natural o jurídica ubicada o con domicilio fuera del territorio colombiano se extralimite o afecte el derecho fundamental al habeas data y a la protección de datos personales la Superintendencia de Industria y Comercio u otra autoridad nacional puede imponer alguna sanción? De ser así ¿de qué tipo sería la sanción?".*

Respuesta: La Superintendencia de Industria y Comercio está facultada para imponer sanciones y/o impartir órdenes a los Responsables y Encargados del Tratamiento que incumplan las disposiciones establecidas en la Ley 1581 de 2012, dentro de ámbito de aplicación de la misma. Las sanciones pueden consistir en multas de carácter pecuniario y/o en la suspensión, o cierre temporal o definitivo de las operaciones relacionadas con el Tratamiento.

13. *"¿Qué otro país del mundo ha declarado a los Estados Unidos como un país con nivel adecuado de protección de datos en los mismos términos que lo hizo la SIC mediante la precitada circular 5 de 2017?".*

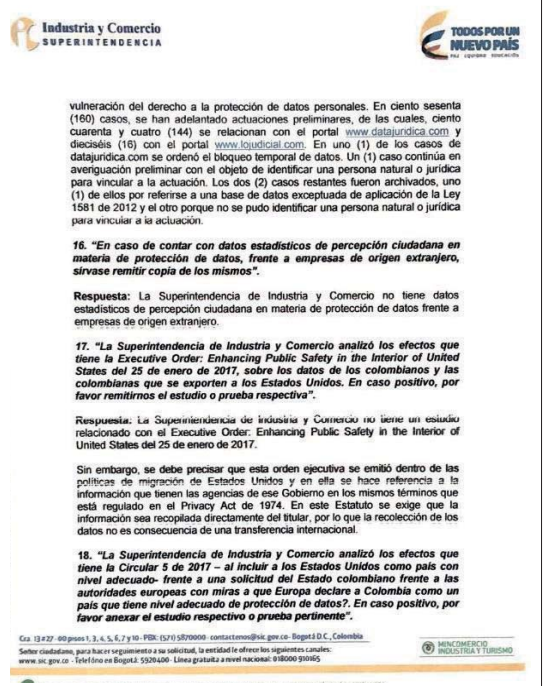
Respuesta: La Unión Europea declaró a Estados Unidos de América un país con nivel adecuado de protección respecto de las empresas certificadas en el marco del Escudo de Privacidad.

14. *"¿Cuáles serían las medidas concretas que dispondría el gobierno de los Estados Unidos en favor de los colombianos en materia de protección de datos?".*

Respuesta: No hay medidas concretas que haya dispuesto el Gobierno de Estados Unidos de América en favor de los colombianos en materia de protección de datos personales. En consecuencia, aplican el régimen legal de privacidad, compuesto por las leyes citadas en precedencia.

15. *"Sírvase informar ¿cuántas denuncias o quejas se han interpuesto en los últimos cinco años contra empresas o personas extranjeras relacionadas con violaciones al derecho fundamental al habeas data y a la protección de los datos personales? ¿Se han iniciado investigaciones por tales hechos? En caso afirmativo ¿cuáles han sido los resultados de esas investigaciones?".*

Respuesta: La Superintendencia de Industria y Comercio ha recibido 163 quejas que involucran a empresas o personas extranjeras, relacionadas con la



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

vulneración del derecho a la protección de datos personales. En ciento sesenta (160) casos, se han adelantado actuaciones preliminares, de las cuales, ciento cuarenta y cuatro (144) se relacionan con el portal www.datajuridica.com y dieciséis (16) con el portal www.lojudicial.com. En uno (1) de los casos de datajuridica.com se ordenó el bloqueo temporal de datos. Un (1) caso continúa en averiguación preliminar con el objeto de identificar una persona natural o jurídica para vincular a la actuación. Los dos (2) casos restantes fueron archivados, uno (1) de ellos por referirse a una base de datos exceptuada de aplicación de la Ley 1581 de 2012 y el otro porque no se pudo identificar una persona natural o jurídica para vincular a la actuación.

16. *"En caso de contar con datos estadísticos de percepción ciudadana en materia de protección de datos, frente a empresas de origen extranjero, sírvase remitir copia de los mismos".*

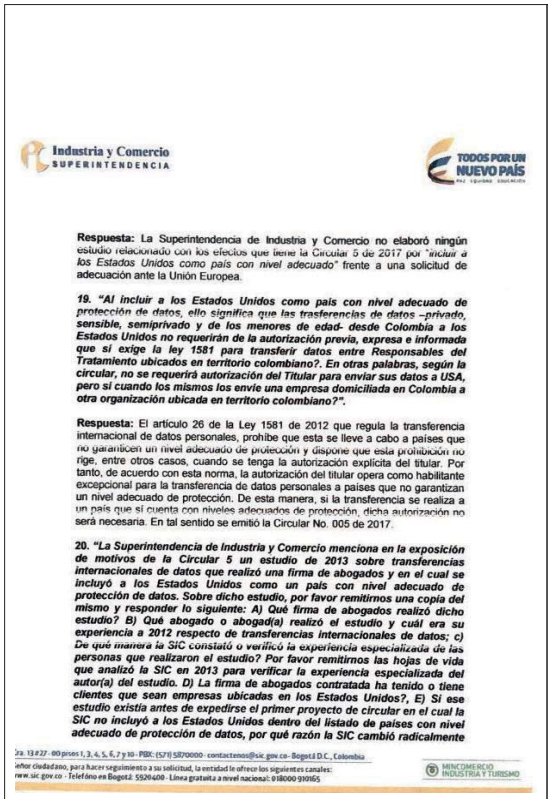
Respuesta: La Superintendencia de Industria y Comercio no tiene datos estadísticos de percepción ciudadana en materia de protección de datos frente a empresas de origen extranjero.

17. *"La Superintendencia de Industria y Comercio analizó los efectos que tiene la Executive Order: Enhancing Public Safety in the Interior of United States del 25 de enero de 2017, sobre los datos de los colombianos y las colombianas que se exporten a los Estados Unidos. En caso positivo, por favor remitirnos el estudio o prueba respectiva".*

Respuesta: La Superintendencia de Industria y Comercio no tiene un estudio relacionado con el Executive Order: Enhancing Public Safety in the Interior of United States del 25 de enero de 2017.

Sin embargo, se debe precisar que esta orden ejecutiva se emitió dentro de las políticas de migración de Estados Unidos y en ella se hace referencia a la información que tienen las agencias de ese Gobierno en los mismos términos que está regulado en el Privacy Act de 1974. En este Estatuto se exige que la información sea recopilada directamente del titular, por lo que la recolección de los datos no es consecuencia de una transferencia internacional.

18. *"La Superintendencia de Industria y Comercio analizó los efectos que tiene la Circular 5 de 2017 – al incluir a los Estados Unidos como país con nivel adecuado- frente a una solicitud del Estado colombiano frente a las autoridades europeas con miras a que Europa declare a Colombia como un país que tiene nivel adecuado de protección de datos?. En caso positivo, por favor anexar el estudio respectivo o prueba pertinente".*



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

Respuesta: La Superintendencia de Industria y Comercio no elaboró ningún estudio relacionado con los efectos que tiene la Circular 5 de 2017 por *"incluir a los Estados Unidos como país con nivel adecuado"* frente a una solicitud de adecuación ante la Unión Europea.

19. "Al incluir a los Estados Unidos como país con nivel adecuado de protección de datos, ello significa que las trasferencias de datos –privado, sensible, semiprivado y de los menores de edad- desde Colombia a los Estados Unidos no requerirán de la autorización previa, expresa e informada que sí exige la ley 1581 para transferir datos entre Responsables del Tratamiento ubicados en territorio colombiano?. En otras palabras, según la circular, no se requerirá autorización del Titular para enviar sus datos a USA, pero sí cuando los mismos los envíe una empresa domiciliada en Colombia a otra organización ubicada en territorio colombiano?".

Respuesta: El artículo 26 de la Ley 1581 de 2012 que regula la transferencia internacional de datos personales, prohíbe que esta se lleve a cabo a países que no garanticen un nivel adecuado de protección y dispone que esta prohibición no rige, entre otros casos, cuando se tenga la autorización explícita del titular. Por tanto, de acuerdo con esta norma, la autorización del titular opera como habilitante excepcional para la transferencia de datos personales a países que no garantizan un nivel adecuado de protección. De esta manera, si la transferencia se realiza a un país que sí cuenta con niveles adecuados de protección, dicha autorización no será necesaria. En tal sentido se emitió la Circular No. 005 de 2017.

20. "La Superintendencia de Industria y Comercio menciona en la exposición de motivos de la Circular 5 un estudio de 2013 sobre transferencias internacionales de datos que realizó una firma de abogados y en el cual se incluyó a los Estados Unidos como un país con nivel adecuado de protección de datos. Sobre dicho estudio, por favor remitirnos una copia del mismo y responder lo siguiente: A) Qué firma de abogados realizó dicho estudio? B) Qué abogado o abogad(a) realizó el estudio y cuál era su experiencia a 2012 respecto de transferencias internacionales de datos; c) De qué manera la SIC constató o verificó la experiencia especializada de las personas que realizaron el estudio? Por favor remitirnos las hojas de vida que analizó la SIC en 2013 para verificar la experiencia especializada del autor(a) del estudio. D) La firma de abogados contratada ha tenido o tiene clientes que sean empresas ubicadas en los Estados Unidos?, E) Si ese estudio existía antes de expedirse el primer proyecto de circular en el cual la SIC no incluyó a los Estados Unidos dentro del listado de países con nivel adecuado de protección de datos, por qué razón la SIC cambió radicalmente *su posición y en la segunda versión del proyecto de circular sí decidió incluir a los Estados Unidos en dicho listado?".*

Respuesta: De acuerdo con su solicitud, se anexa copia del *"Estudio sobre la aplicación en Colombia de las normas sobre transferencias de datos personales"*.

De otra parte, en relación con las preguntas formuladas, manifestamos lo siguiente:

a. El estudio fue elaborado por la sociedad Valbuena Abogados S.A.S.

b. El proponente es una persona jurídica que, de acuerdo con lo establecido en el Pliego de Condiciones definitivo del Concurso de Méritos de Lista Corta No. SIC 94 de 2013, adelantado por la Superintendencia de Industria y Comercio con el objeto de contratar el estudio mencionado, presentó un equipo de trabajo conformado por Gustavo Valbuena Quiñones como Director del Proyecto y María Fernanda de la Ossa como Profesional de apoyo.

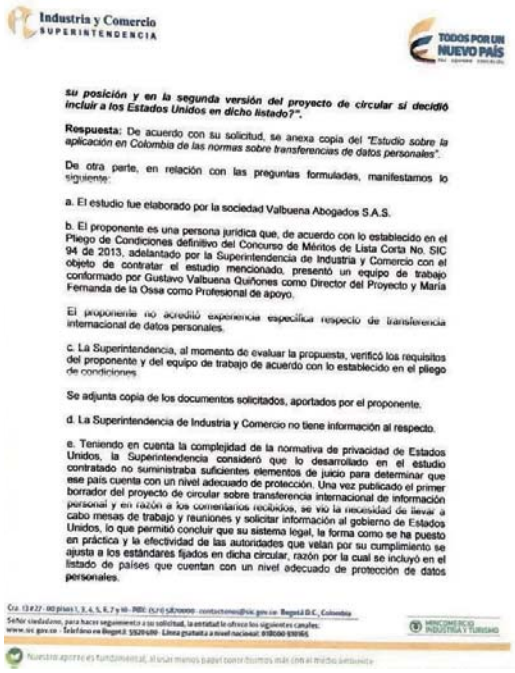
El proponente no acreditó experiencia específica respecto de transferencia internacional de datos personales.

c. La Superintendencia, al momento de evaluar la propuesta, verificó los requisitos del proponente y del equipo de trabajo de acuerdo con lo establecido en el pliego de condiciones.

Se adjunta copia de los documentos solicitados, aportados por el proponente.

d. La Superintendencia de Industria y Comercio no tiene información al respecto.

e. Teniendo en cuenta la complejidad de la normativa de privacidad de Estados Unidos, la Superintendencia consideró que lo desarrollado en el estudio contratado no suministraba suficientes elementos de juicio para determinar que ese país cuenta con un nivel adecuado de protección. Una vez publicado el primer borrador del proyecto de circular sobre transferencia internacional de información personal y en razón a los comentarios recibidos, se vio la necesidad de llevar a cabo mesas de trabajo y reuniones y solicitar información al gobierno de Estados Unidos, lo que permitió concluir que su sistema legal, la forma como se ha puesto en práctica y la efectividad de las autoridades que velan por su cumplimiento se ajusta a los estándares fijados en dicha circular, razón por la cual se incluyó en el listado de países que cuentan con un nivel adecuado de protección de datos personales.



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

21. "Teniendo en cuenta lo que dice el parágrafo primero del numeral 3.2 de la Circular respecto del principio de responsabilidad demostrada, por favor responder lo siguiente: a) Cuáles son las medidas efectivas y apropiadas que debe adoptar el Responsable del tratamiento de datos para garantizar en los Estados Unidos el adecuado tratamiento de los datos personales que son exportados desde Colombia a dicho país? B) Esas medidas son suficientes para dar plena certeza al ciudadano colombiano que sus datos serán tratados debidamente en los Estados Unidos y que sus derechos serán plenamente respetados en dicho país?. Por favor explicar su respuesta en caso que sea afirmativa. C) Por qué la SIC no menciona en la circular las medidas concretas que se deben adoptar en virtud del principio de responsabilidad demostrada y deja el tema en manos de cada Responsable del tratamiento? D) No cree la SIC que la ausencia de dichas medidas en la circular dejará al arbitrio de cada Responsable el nivel de protección y garantía de los derechos de los titulares de los datos que son exportados desde Colombia a los Estados Unidos?

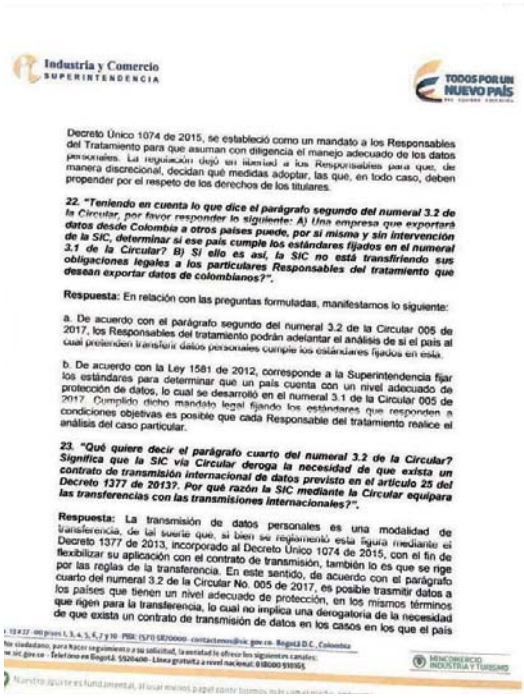
Respuesta: En relación con las preguntas formuladas, manifestamos lo siguiente:

a. Las medidas efectivas y apropiadas que debe adoptar el Responsable del Tratamiento son las necesarias (i) para garantizar el adecuado uso de los datos que transfiere, teniendo en cuenta la naturaleza de los mismos y los riesgos potenciales que la transferencia puede causar sobre los derechos de los titulares y (ii) otorgar seguridad a los registros al momento de efectuar dicha transferencia, las cuales, de acuerdo con el principio de responsabilidad demostrada corresponde a cada Responsable del tratamiento implementar.

b. Para determinar que las medidas adoptadas son suficientes, es preciso que el Responsable del tratamiento tenga en cuenta las condiciones particulares de la transferencia de datos personales que pretende realizar y analice los riesgos asociados a la operación para definir los controles o medidas que debe implementar con el fin de mitigar los riesgos identificados y brindar las garantías necesarias frente al respeto de los derechos de los Titulares.

c. La Superintendencia de Industria y Comercio no establece medidas específicas a cargo de los Responsables del Tratamiento por cuanto le corresponde a quien recoge y hace tratamiento de datos personales determinar, en el marco de una debida diligencia, las medidas que le permitan asegurar de manera efectiva el adecuado tratamiento de los datos.

d. La implementación de medidas efectivas y apropiadas en desarrollo del principio de responsabilidad demostrada, en las condiciones previstas en el



Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

Decreto Único 1074 de 2015, se estableció como un mandato a los Responsables del Tratamiento para que asuman con diligencia el manejo adecuado de los datos personales. La regulación dejó en libertad a los Responsables para que, de manera discrecional, decidan qué medidas adoptar, las que, en todo caso, deben propender por el respeto de los derechos de los titulares.

22. "Teniendo en cuenta lo que dice el parágrafo segundo del numeral 3.2 de la Circular, por favor responder lo siguiente: A) Una empresa que exportará datos desde Colombia a otros países puede, por sí misma y sin intervención de la SIC, determinar si ese país cumple los estándares fijados en el numeral 3.1 de la Circular? B) Si ello es así, la SIC no está transfiriendo sus obligaciones legales a los particulares Responsables del tratamiento que deseen exportar datos de colombianos?".

Respuesta: En relación con las preguntas formuladas, manifestamos lo siguiente:

a. De acuerdo con el parágrafo segundo del numeral 3.2 de la Circular 005 de 2017, los Responsables del tratamiento podrán adelantar el análisis de si el país al cual pretenden transferir datos personales cumple los estándares fijados en esta.

b. De acuerdo con la Ley 1581 de 2012, corresponde a la Superintendencia fijar los estándares para determinar qué un país cuenta con un nivel adecuado de protección de datos, lo cual se desarrolló en el numeral 3.1 de la Circular 005 de 2017. Cumplido dicho mandato legal fijando los estándares que responden a condiciones objetivas es posible que cada Responsable del tratamiento realice el análisis del caso particular.

23. "Qué quiere decir el parágrafo cuarto del numeral 3.2 de la Circular? Significa que la SIC vía Circular deroga la necesidad de que exista un contrato de transmisión internacional de datos previsto en el artículo 25 del Decreto 1377 de 2013?. Por qué razón la SIC mediante la Circular equipara las transferencias con las transmisiones internacionales?".

Respuesta: La transmisión de datos personales es una modalidad de transferencia, de tal suerte que, si bien se reglamentó esta figura mediante el Decreto 1377 de 2013, incorporado al Decreto Único 1074 de 2015, con el fin de flexibilizar su aplicación con el contrato de transmisión, también lo es que se rige por las reglas de la transferencia. En este sentido, de acuerdo con el parágrafo cuarto del numeral 3.2 de la Circular No. 005 de 2017, es posible trasmitir datos a los países que tienen un nivel adecuado de protección, en los mismos términos que rigen para la transferencia, lo cual no implica una derogatoria de la necesidad de que exista un contrato de transmisión de datos en los casos en los que el país

Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

al que se va a remitir la información no cuente con un nivel adecuado de protección.

24. *"Qué significa en concreto el parágrafo del numeral 3.3. de la Circular Externa 5 del 10 de agosto de 2017".*

Respuesta: El parágrafo del numeral 3.3 de la Circular Externa No. 005 de 2017 establece las condiciones para que los Responsables del Tratamiento lleven a cabo la transferencia internacional de datos personales bajo la presunción de que la operación es viable y que cuenta con declaración de conformidad. El cumplimiento de estas condiciones podrá ser verificado por la Superintendencia de Industria y Comercio en cualquier momento y en caso de que no se ajusten a lo establecido podrá adelantar la respectiva investigación e imponer las sanciones o tomar las medias que correspondan.

25. *"La Superintendencia de Industria y Comercio contrató algún asesor externo para redactar la Circular 5 de 2017?. En caso positivo, a) de qué manera la SIC constató o verificó la experiencia especializada en transferencias internacionales de la persona contratada? Por favor remitirnos la hoja de vida que analizó la SIC para contratar dicha persona. b) La persona o firma contratada ha tenido o tiene clientes que sean empresas ubicadas en los Estados Unidos?. c) La persona o firma contratada ha tenido o tiene clientes que se dediquen a ofrecer servicios relacionados con el Principio de responsabilidad demostrada o Accountability?".*

Respuesta: La Superintendencia de Industria y Comercio no se contrató ningún asesor externo para redactar la Circular Externa 005 de 2017.

Sírvanse contar con este Despacho para cualquier aclaración sobre el particular.

Del H. Senador,

PABLO FELIPE ROBLEDO DEL CASTILLO
Superintendente de Industria y Comercio

Anexo (1) CD

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

TABLA DE CONTENIDO

Valbuena ABOGADOS

"La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los operadores que haga parte del banco de datos que administra, podrá ser entregada de manera verbal, escrita, o puesta a disposición de las siguientes personas y en los siguientes términos:

f) A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. **Si el receptor de la información fuere un banco de datos extraniero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular.**" (Subrayas y negrillas fuera del texto)

En relación con la citada norma, la Corte Constitucional mediante sentencia C-1011 de 2008 que estudió la constitucionalidad de la ley estatutaria del mismo año precisó lo siguiente:

"(...) Para cumplir con esta obligación de protección y garantía de los derechos del sujeto concernido, el legislador estatutario estableció en el artículo 17 que las Superintendencias de Industria y Comercio y Financiera ejercerán la función de vigilancia de los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto refiere a la administración de datos personales regulada por la normatividad objeto de estudio. **Estas funciones de vigilancia consisten, entre otros aspectos, en impartir instrucciones y órdenes sobre la manera como deben cumplirse las disposiciones previstas por la normatividad estatutaria, relacionadas con la administración de la mencionada información, para lo cual las Superintendencias fijarán los criterios que faciliten su cumplimiento y señalarán procedimientos para su cabal aplicación.**

Previsiones estatutarias de esta naturaleza tienen, a juicio de la Corte, efectos concretos en la interpretación de las posibilidades de transmisión internacional de datos personales previstos en el literal f) del artículo 5º. En efecto, la interpretación aislada del precepto llegaría a concluir **que la verificación sobre la existencia en la legislación del banco de datos de**

Valbuena ABOGADOS

destino de garantías suficientes para la protección de los derechos del titular, es una materia que depende única y exclusivamente de la voluntad y libre evaluación del operador nacional. Empero, esta lectura se muestra errónea y descontextualizada, puesto que desconoce que el legislador estatutario ha instituido que las autoridades del Estado que ejercen la función de vigilancia no están limitadas al ejercicio del derecho administrativo sancionador, sino que también están investidas de la facultad de impartir instrucciones y órdenes para el cumplimiento de la ley, lo que significa que estas autoridades deberán indicar los parámetros específicos para que la actuación de los operadores sea en todo compatible con la protección de los derechos fundamentales del titular de la información.

En este orden de ideas, si el legislador estatutario ha señalado que las Superintendencias de Industria y Comercio y Financiera, de acuerdo con las competencias previstas en el ordenamiento, tienen la competencia para señalar el modo particular y específico en que deberán cumplirse las disposiciones de la normatividad estatutaria; entonces estas entidades deberán determinar los parámetros que deberá tener en cuenta el operador nacional para la verificación de que la legislación aplicable al banco de datos de destino ofrece garantías suficientes para la protección de los derechos del titular. En ese sentido, las citadas Superintendencias deberán analizar el cumplimiento de los estándares de garantía de derechos predicables del titular del dato personal, en la legislación del banco de datos extranjero de destino. Así, dichas entidades podrán, inclusive, identificar expresamente los ordenamientos legales extranjeros respecto de los cuales, luego de un análisis suficiente, pueda predicarse dicho grado de protección suficiente de los derechos del sujeto concernido. De manera correlativa, el ejercicio del acto de verificación a cargo del operador nacional al que refiere el literal f) del artículo 5º del Proyecto de Ley, estará supeditado a que las entidades que ejercen la función de vigilancia hayan realizado el análisis de cumplimiento de estándares de protección de derechos antes aludido." (Subrayas y negrillas fuera del texto).

Vemos entonces que con anterioridad a la expedición de la Ley 1581 de 2012, Colombia no contaba con normas que regularan la manera en que debían efectuarse las transferencias internacionales de datos. Salvo lo dispuesto por el literal f) del artículo 5 de la Ley 1266 de 2008 mencionado con la aclaración hecha por la Corte en citada sentencia,

las transferencias internacionales de datos en el marco de la regulación sectorial contenido en la ley (esto es, información financiera, crediticia, comercial, de servicios y la proveniente de terceros países), debían efectuarse teniendo en cuenta los parámetros fijados por la Superintendencia de Industria y Comercio y la Superintendencia Financiera de Colombia dentro de la órbita de sus competencias.

Al respecto, vale la pena destacar la importancia que la Corte misma reconoce a este aspecto de la protección del derecho fundamental del artículo 15 de la Constitución Política. La verificación del cumplimiento de las garantías en materia de protección de datos, en el marco de una transferencia internacional, no puede quedar sujeta a la mera discrecionalidad del operador de información. Es la autoridad estatal quien debe establecer parámetros claros al respecto.

Ahora bien, con la entrada en vigencia de la Ley 1581 de 2012 se señala un marco expreso dentro del cual resulta procedente la realización de transferencias internacionales de datos. Así, el artículo 26 de la mencionada norma, que se verá más adelante en detalle, parte de la premisa general de prohibir la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Lo anterior, tal como lo precisó la Corte Constitucional en sentencia C-748 de 2011, mediante la cual se analizó la constitucionalidad de la referida ley 1581 del mismo año, "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."

Al respecto, el artículo 26 de la Ley 1581 de 2012 establece que:

> "Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.
>
> Esta prohibición no regirá cuando se trate de:
>
> a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;
>
> b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento

del Titular por razones de salud o higiene pública;

c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;

d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;

e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;

f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Parágrafo 1°. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Parágrafo 2°. Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008."

Tal como con claridad lo determinó la Corte, cuando el país destinatario de la transferencia no tiene un nivel de protección adecuado pero concurre alguna de las circunstancias previstas en los literales a) a f) del artículo 26 de la ley 1581 de 2012, podrá realizarse la transferencia.

Es importante precisar que el régimen de protección previsto en el artículo 26 de la Ley 1581 de 2012, está fundado sobre la existencia de "niveles adecuados de protección", concepto que se articula sobre dos elementos: uno material y otro de garantía.

a) **El elemento material** se construye sobre la existencia de unos principios básicos de

protección. Cualquier tratamiento de datos por parte de un sujeto de derecho público o privado debe respetar fundamentalmente los principios de finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. De otra parte, el elemento material exige el establecimiento de un catálogo de derechos consagrados en favor del titular de la información. Estos derechos deben permitir como mínimo el acceso, rectificación, y supresión de los datos personales recolectados.

b) **El elemento de garantía** hace referencia al establecimiento de mecanismos que faciliten el ejercicio de los derechos de los titulares de información frente a los responsables y encargados del tratamiento, lo que implica la existencia de una infraestructura para la garantía y control de esos derechos (Artículos 14 y 15 de la Ley 1581 de 2012). Este elemento de garantía procesal contempla además, mecanismos de sanción al responsable por parte de la autoridad de protección (Artículo 23 Ley 1581 de 2012).

Estos dos elementos fueron claramente puestos de presente por la Corte Constitucional al analizar la exequibilidad de la regulación estatutaria. Al precisar el alcance de la expresión "niveles adecuados de protección de datos", la Corte indicó como criterio para determinar si un país cuenta con elementos suficientes para garantizar un nivel adecuado de protección de datos la necesidad de verificar si "su legislación cuenta; con unos principios, que abarquen las obligaciones y derechos de las partes (titular del dato, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos de datos personales), y de los datos (calidad del dato, seguridad técnica) y; con un procedimiento de protección de datos que involucre mecanismos y autoridades que efectivicen la protección de la información. De lo anterior se deriva que el país al que se transfiera los datos, no podrá proporcionar un nivel de protección inferior al contemplado en este cuerpo normativo que es objeto de estudio".

Sobre el particular, vale la pena advertir que, tal como lo recoge la Corte en su decisión, la expresión "nivel adecuado de protección" apareció en el marco de los trabajos del Grupo de Protección de las Personas en lo que respecta al tratamiento de Datos Personales de la Directiva 95/46/CE (en adelante referido como "Grupo") al establecer las reglas para la transferencia de datos personales a terceros países. El Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE y se trata del órgano consultivo independiente de la Unión Europea sobre protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE[1] y en el artículo 14 de la Directiva 97/66/CE[2].

[1] Los artículos 29 y 30 de la Directiva 95/46/CE establecen lo siguiente:

"Artículo 29: Grupo de protección de las personas en lo que respecta al tratamiento de datos personales.

1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado «Grupo».
2. Dicho Grupo tendrá carácter consultivo e independiente.

El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión. Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios.

3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control.

4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable.

5. La Comisión desempeñará las funciones de secretaría del Grupo.

6. El Grupo aprobará su reglamento interno.

7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de éste, bien previa solicitud de un representante de las autoridades de control, bien a solicitud de la Comisión".

"Artículo 30:

1. El Grupo tendrá por cometido:

a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;

c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;

d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

2. Si el Grupo comprobare la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión.

3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.

4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión y al Comité contemplado en el artículo 31.

5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado.

6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado".

[2] **DIRECTIVA 97/66/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en EL sector de las telecomunicaciones que los datos personales puedan circular libremente en la Comunidad.** ARTÍCULO 14 NUMERAL 3:. El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido con arreglo al artículo 29 de la Directiva 95/46/C Ejercerá las funciones especificadas en el artículo 30 de la citada Directiva también por lo que se refiere a la

En desarrollo de su mandato, el Grupo adoptó dos documentos: (i) Documento adoptado por el Grupo de Trabajo el 26 de junio de 1997 Primeras Orientaciones sobre la Transferencia de Datos personales a Terceros Países y las Posibles formas de evaluar la adecuación y, (ii) Documento de Trabajo Transferencias de Datos Personales a Terceros Países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE aprobado por el Grupo de Trabajo el 24 de julio de 1998.

En efecto, mediante documento adoptado el 26 de junio de 1997 se establecieron las primeras orientaciones sobre la transferencia de datos personales a países terceros y las posibles formas de evaluar la adecuación. Como objetivo del citado documento se planteó en forma expresa:

"Este documento no tiene por objetivo tratar todas las cuestiones que surgen en relación con la Directiva respecto a la transferencia de datos personales a países terceros, sino que más bien pretende centrarse en la cuestión de evaluar la adecuación en el sentido de los apartados 1 y 2 del artículo 25. El alcance de las excepciones al requisito del "nivel de protección adecuado" del apartado 1 del artículo 26 no se consideran en este documento. La hipótesis de trabajo es que la formulación de estas exenciones es bastante limitada, y que probablemente habrá un gran número de casos que caigan fuera de su alcance y que deban por lo tanto ser objeto de una evaluación de su adecuación. El Grupo de Trabajo examinará el alcance exacto de estas excepciones en el futuro.[3]".

A su vez, mediante documento aprobado por el Grupo el 24 de julio de 1998, se establecieron los criterios de aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea. El objetivo de este documento se contrae a "reunir el trabajo previamente realizado por el Grupo de Trabajo de los Comisarios para la Protección de Datos de la UE, creado al amparo del artículo 29 de la Directiva sobre protección de datos, en un conjunto de reflexiones más exhaustivo sobre todas las cuestiones centrales planteadas en las transferencias de datos personales a terceros

protección de los derechos y libertades fundamentales y de los intereses legítimos en el sector de las telecomunicaciones, que son objeto de la presente Directiva.

[3] COMISIÓN EUROPEA DIRECCIÓN GENERAL XV Mercado Interior y Servicios Financieros Libre circulación de la información, Derecho de sociedades e información financiera Libre circulación de la información, protección de datos y sus aspectos internacionales GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Primeras orientaciones sobre la transferencia de datos personales a países terceros - Posibles formas de evaluar la adecuación Documento de debate adoptado por el Grupo de Trabajo el 26 de junio de 1997

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

países en el contexto de la aplicación de la Directiva sobre protección de datos de la UE (95/46/CE)."[4]

En los documentos antes mencionados, el Grupo estableció que un nivel de protección adecuado depende de varios factores; unos de naturaleza material y otros de carácter institucional (requisitos de procedimiento). Los primeros, básicamente se vinculan con un catálogo de derechos que se deben reconocer al titular de los datos personales y una serie de obligaciones para quienes realizan actividades de tratamiento. Los segundos comprenden mecanismos y procedimientos que garanticen la efectividad de las normas y sancionen su incumplimiento.

En particular frente a los mecanismos de protección se considera necesaria la existencia de una autoridad independiente que no sólo controle, vigile y, de ser el caso sancione a quienes realizan tratamiento de datos personales, sino que reciba las quejas de los ciudadanos e inicie las investigaciones pertinentes como garante de la protección de estos datos[5].

El mencionado Grupo, también a partir de lo contenido en la Directiva 95/46/CE, el Convenio 108 de 1981, las directrices de la Organización para la Cooperación y el Desarrollo Económico OCDE de 1980 y los principios de la ONU de 1990, referencias normativas y de principios a las que más adelante nos referiremos, fijó una serie de las

[4] COMISIÓN EUROPEA DIRECCIÓN GENERAL XV Mercado Interior y Servicios Financieros Libre Circulación de la Información, Derecho de Sociedades e Información Financiera Libre Circulación de la Información, protección de datos y sus aspectos internacionales Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998

[5] COMISIÓN EUROPEA DIRECCIÓN GENERAL XV Mercado Interior y Servicios Financieros Libre Circulación de la Información, Derecho de Sociedades e Información Financiera Libre Circulación de la Información, protección de datos y sus aspectos internacionales Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998: Los objetivos de un sistema de protección de datos son básicamente tres: 1) Ofrecer un **nivel satisfactorio de cumplimiento** de las normas. (Ningún sistema puede garantizar el 100 % de cumplimiento, pero algunos son mejores que otros). Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos. 2) Ofrecer **apoyo y asistencia a los interesados** en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente. 3) Ofrecer **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas. Este es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

básicas comunes para determinar si las normas de un determinado país brindan un nivel adecuado de protección[6].

Se observa entonces que el modelo europeo de protección de datos insta a los Estados a establecer dentro de sus ordenamientos unos principios mínimos que han de regir el manejo de la información de datos, y por tanto, la interpretación de las normas internas de cada Estado debe hacerse de conformidad con estos estándares de protección. En relación con este modelo de protección la Corte Constitucional, en la misma sentencia C-748 de 2011 que se ocupó del análisis de exequibilidad de la ley 1581 precisó:

> "Europa ha sido considerada pionera en establecer fórmulas jurídicas tendientes a la protección de datos cuando se transfieren a terceros países. Así, uno de los presupuestos exigidos para que se pueda realizar la transferencia es que el país receptor cuente con un **adecuado nivel de protección** a la luz del estándar europeo. (...)
>
> En relación con el ahora proyecto de Ley que es objeto de estudio, debe decirse en primer lugar que difiere de lo señalado en la Ley 1266 de 2008, pero **coincide con el modelo europeo, en cuanto otorga la competencia de determinar qué países proporcionan un nivel adecuado de protección de datos en el órgano de control, esto es, la Superintendencia de Industria y Comercio, y no en los operadores que manejan los datos**.
>
> En consecuencia, e inclusive, integrando lo contemplado en la Ley 1266 de 2008, por disposición del parágrafo 2º del artículo 26 del Proyecto de Ley en estudio, será la Superintendencia de Industria y Comercio la encargada de determinar si un país otorga garantías de protección de datos.

[6] COMISIÓN EUROPEA DIRECCIÓN GENERAL XV Mercado Interior y Servicios Financieros Libre Circulación de la Información, Derecho de Sociedades e Información Financiera Libre Circulación de la Información, protección de datos y sus aspectos internacionales Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998: El objetivo de la protección de datos es ofrecer protección a las personas cuyos datos son objeto de tratamiento. Normalmente, dicho objetivo se logra combinando los derechos del interesado **y las obligaciones de quienes tratan los datos o controlan dicho tratamiento. Las obligaciones y los derechos establecidos en la Directiva 95/46/CE se basan en aquellos dispuestos en el Convenio nº 108 (1981) del Consejo de Europa, que a su vez no son diferentes de los incluidos en las directrices de la OCDE (1980) o en las directrices de la ONU(90). Por eso, parece que existe un alto grado de consenso en relación con el contenido de las normas de protección de datos que traspasa los límites del espacio ocupado por los quince estados de la Comunidad**

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

> **En este sentido, y con sujeción a lo indicado por el referido Grupo de Trabajo de Protección de Datos de la Unión Europea, se entenderá que 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 involucre mecanismos y autoridades que efectivicen la protección de la información. De lo anterior se deriva que el país al que se transfiera los datos, no podrá proporcionar un nivel de protección inferior al contemplado en este cuerpo normativo que es objeto de estudio.**" (Subrayas y negrillas fuera del texto).

En consideración a lo anterior, resulta claro que el modelo adoptado por la legislación colombiana en materia de transferencia internacional de datos, parte de los presupuestos consagrados por el Grupo que se encuentran principalmente contenidos en el Documento de Trabajo Transferencias de Datos Personales a Terceros Países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo el 24 de julio de 1998 y que serán explicados con detalle en el siguiente capítulo.

2. MEJORES PRÁCTICAS ACEPTADAS INTERNACIONALMENTE EN MATERIA DE TRANSFERENCIA Y TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES Y ALCANCE DE LA EXIGENCIA "NIVEL ADECUADO DE PROTECCIÓN"

A continuación procedemos a efectuar una descripción general de las reglas sobre protección de datos personales expedidas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), las proferidas por la Organización de las Naciones Unidas, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión y las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana, específicamente las relacionadas con la circulación transfronteriza de información personal, que en esta materia, esto es, en lo relacionado con transferencia y transmisión internacionales de datos constituyen estándares fundamentales de protección de datos personales y de privacidad.

2.1. Organización para la Cooperación y el Desarrollo Económicos (OCDE)

El Consejo de la Organización para la Cooperación y el Desarrollo Económico ("OCDE")

aprobó como una recomendación el primer instrumento internacional propuesto para reglamentar el procesamiento de datos personales y el flujo internacional de dichos datos en 1980 a través de una serie de directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales[7]. Estas reglas sugeridas pretenden garantizar la protección de los derechos individuales incursos en los procesos de transferencia de datos al tiempo que buscan promover la democracia, el respeto por los derechos humanos y la economía de libre mercado. Las directrices establecen un estándar mínimo a efectos de promover la armonización internacional de las normas relativas al tratamiento manual y automatizado de información personal por los sectores público y privado.

Así, desde el preámbulo de las Directrices que rigen la protección de la intimidad y la circulación transfronteriza de datos de carácter personal, aprobadas el 23 de septiembre de 1980 (las "Directrices"), el Consejo de la OCDE ya reconoce expresamente que "la circulación transfronteriza de datos personales contribuye al desarrollo económico y social", pero al propio tiempo recuerda que "la legislación nacional relativa a la protección de la intimidad y de la circulación transfronteriza de datos personales puede obstaculizar tal circulación transfronteriza".

Las Directrices establecen los principios básicos vinculados a la protección de datos personales. A través de estas Directrices, la OCDE delimita estos principios, enumerando como básicos los siguientes:

1. Principio de limitación de la recogida
2. Principio de calidad de los datos
3. Principio de especificación de la finalidad
4. Principio de limitación de uso
5. Principio de salvaguardas de seguridad
6. Principio de apertura de los datos
7. Principio de participación individual
8. Principio de responsabilidad

Respecto del flujo transfronterizo de datos personales las Directrices proponen en últimas

[7] Recomendación del Consejo de la OCDE relativa a las Directrices que rigen la protección de la intimidad y la circulación transfronteriza de datos de carácter personal, aprobada el 23 de septiembre de 1980.

un balance. Por un lado, evitan la adopción de medidas que establezcan obstáculos innecesarios al libre flujo de información y, por el otro, restringen el flujo cuando un país no provee un nivel de protección "equivalente".

Así, el artículo 17 de las Directrices establece lo siguiente:

> "La circulación transfronteriza de datos personales entre dos países miembros no debería restringirse, salvo en el caso de que el segundo país aun no haya observado sustancialmente estas Directrices o cuando la reexportación de tales datos soslayase su legislación nacional sobre la intimidad. Cualquier país miembro también podrá imponer restricciones respecto a ciertas categorías de datos personales para las cuales su legislación nacional sobre la intimidad incluya normativas específicas en vista de la índole de tales datos y para las cuales otro país miembro no proporcione protección equivalente.

Paralelamente, la OCDE ha adoptado varias directrices en asuntos relacionados con la protección de los datos personales, tales como transparencia pública y acceso a la información [8], privacidad en redes globales [9] y comunicaciones electrónicas no solicitadas[10].

Sin embargo, la eficacia de las directrices de la OCDE es limitada por su propia naturaleza, pues al ser recomendaciones se trata de un documento jurídicamente no vinculante y por consiguiente, sin posibilidad de cumplimiento obligatorio.

2.2. Asia Pacific Economic Cooperation (APEC) Privacy Framework:

Asia Pacific Economic Cooperation (APEC) es un foro multilateral de negociación en temas relativos al intercambio comercial, coordinación y cooperación entre las economías de los países que la integran, orientado a promover y facilitar el comercio, las inversiones, la cooperación económica y técnica entre los mismos. Creado en 1989 incluye países como Australia, Canadá, Corea, Chile, Estados Unidos de América, Filipinas, Indonesia, Japón,

[8] Organization for Economic Co-operation and Development, Declaration on Transborder Data Flows, adopted by the Governments of OECD Member countries on 11 April 1985 - C(85)139

[9] Organization for Economic Co-operation and Development, Declaration on the Protection of Privacy on Global Networks, adopted by the Governments of OECD Member countries on 8 October 1998 - C(98)177.

[10] Organization for Economic Co-operation and Development, Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam, adopted by the Council on 13 April 2006 - C(2006)57.

México, Nueva Zelandia, Perú, Rusia y Vietnam.

APEC Privacy Framework es el documento marco para la regulación del tratamiento de la información personal adoptado por las economías que integran el APEC, mediante el cual se procura el establecimiento de un estándar de protección que no implique trabas para el comercio internacional entre los países miembros. A este respecto, se advierte que el Foro de Cooperación Económica Asia Pacífico (APEC) aprobó en noviembre de 2004 su Marco de Privacidad, con el ánimo de fortalecer la protección de la privacidad y permitir los intercambios de información. Es un programa de voluntario, recíproco, multilateral y de cumplimiento de medidas de seguridad en materia de transferencias transfronterizas de empresas en la región de APEC.

El documento está inspirado también en las directivas de 1980 de la OCDE, y tiene como propósito proveer unos principios generales que guíen la regulación interna de las economías de Asia, en relación con la recolección de información personal que recogen las diferentes entidades públicas o privadas y las transferencias electrónicas que se realicen entre los países miembros del APEC. Sin embargo, la aplicación de dicho marco es de carácter flexible, considerando las diferencias culturales, económicas y legales de cada economía.

Vale la pena resaltar que el APEC Privacy Framework enfatiza las facultades normativas y de control con las que deben contar las entidades responsables del tratamiento de datos y mira con recelo la intervención de una autoridad pública en la materia, por cuanto podría entorpecer el comercio entre las economías involucradas. De hecho, se observa que el estándar de protección previsto en el APEC es menor al previsto por las directrices de la OCDE en 1980.

Establecido lo anterior, a continuación se explican los principios contenidos en el "APEC Privacy Framework" exponiendo sus similitudes con los principios que en Colombia se desprenden de la ley 1581 de 2012 :

a. Prevención de Daño: Este principio se refiere a la prevención del mal uso o indebida recolección de la información personal con el objetivo de impedir causar daño a los titulares de la información. Así, las regulaciones de los países miembros del APEC deben estar orientadas a tomar las medidas conducentes a impedir que se genere un perjuicio para los titulares de la información por su indebida recolección o mal uso.

En Colombia, en el régimen de protección de datos personales previsto en la Ley 1581 de 2012, este postulado corresponde con los principios de circulación restringida y seguridad previstos en los literales f) y g) del artículo 4 que de una parte, señalan que los datos no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley y de la otra obligan a responsables y encargados del tratamiento a manejar los datos personales con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

b. Noticia: Los controladores de la información deben proveer a los titulares de los datos, documentos claros y fácilmente accesibles que den cuenta de sus prácticas y políticas respecto del tratamiento de datos personales. Estos documentos deben incluir: El hecho de que la información está siendo recolectada; los propósitos para los cuales la información es recolectada; los tipos de personas u organizaciones frente a las cuales la información será revelada; la identidad y dirección del controlador de la información; y las alternativas que el controlador de la información ofrece a los individuos relativas al derecho a limitar el uso o revelación de la información, así como los derechos que tienen los titulares de acceder y corregir su información. Se anota que toda esta documentación deberá ser provista antes de la recolección de información, durante la recolección, o inclusive inmediatamente después de la recolección.

   En la Ley 1581 de 2012 este postulado equivale al principio de transparencia previsto en el literal e) del artículo 4, de conformidad con el cual en el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

c. Limitación a la recolección: La recolección de datos personales se deberá limitar a los propósitos de dicha recolección y deberá ser realizada de acuerdo con la ley y obteniendo el consentimiento del titular.

   En el régimen de habeas data colombiano, este postulado corresponde a los principios de finalidad y libertad, postulados estructurales de nuestro sistema de

protección de datos. Así, de conformidad con tales principios el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular y el tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

d. Usos de la Información Personal: Los usos que se le deberán dar a la información recogida deberán ser exclusivamente los que se requieran para lograr los propósitos de la recolección u otros propósitos conexos. Se exceptúan de esta regla general, los casos que se refieren a cuando el titular ha expresado su consentimiento para que se le dé un uso diferente a sus datos personales; cuando es necesario proveer un servicio o producto requerido por el mismo titular de la información; cuando la autoridad competente, una ley o un pronunciamiento judicial así lo determinen.

Estos postulados, a su vez, en nuestra legislación corresponden con los principios de finalidad y libertad consagrados en el artículo 4 de la Ley 1581 de 2012.

e. Escogencia: Los titulares de la información tienen derecho a ser provistos de mecanismos claros, accesibles y fáciles de entender, que les permitan escoger entre si quieren o no que se revele la información recolectada.

Este principio en el régimen de protección colombiano está consagrado como un derecho radicado a favor de los titulares de la información. Así, los titulares de la información, de acuerdo con lo previsto en el artículo 8 de la Ley 1581 de 2012 tienen derecho a, entre otros aspectos a conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o los Encargados, solicitar prueba de la autorización otorgada; ser informado por el Responsable o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales; revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

f. Integridad de la Información: Hace referencia a que la información deba ser exacta, completa y recolectada únicamente hasta la fecha necesaria para que se logren cumplir los propósitos para los cuales se recabó.

Este principio en Colombia, equivale al principio de veracidad o calidad, previsto en el literal d) del artículo 4 de la Ley 1581 de 2012 de conformidad con el cual la información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

g. Garantía de Seguridad: Los controladores de la información deben proteger la información personal con las medidas necesarias para evitar riesgos como pérdida, destrucción, uso, modificación y revelación indebida. Estas medidas deberán ser proporcionales dependiendo del grado de sensibilidad de la información.

En Colombia este postulado corresponde al principio de seguridad de los datos consagrado en el literal g) del artículo 4 de la Ley 1581 de 2012.

h. Acceso y Corrección: Estos principios consisten en el derecho que tiene el titular de que el controlador de la información le confirme si en efecto tiene o no datos personales suyos; en el derecho que tiene el titular de ser informado respecto de su información en un tiempo razonable, sin costo o con uno no excesivo, de una manera razonable y en una forma fácilmente entendible; y en el derecho a rectificar, completar o eliminar sus datos personales de las bases de datos en las que reposan.

Este principio está consagrado en nuestra legislación como un derecho- artículo 21 del Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2012, de acuerdo con el cual los responsables y encargados del tratamiento deben establecer mecanismos sencillos y ágiles que se encuentren permanentemente disponibles a los Titulares con el fin de que estos puedan acceder a los datos personales que estén bajo el control de aquellos y ejercer sus derechos sobre los mismos.

i. Responsabilidad: El controlador de la información será responsable de contar con las medidas adecuadas que den cumplimiento a los principios establecidos en el APEC. Adicionalmente, cuando la información personal vaya a ser transferida a una organización dentro del mismo país o a una organización por fuera del país, el controlador de la información deberá obtener el consentimiento del titular de los datos, o asegurarse de que la organización a la cual se realizará la transferencia, cumpla con los principios a los que se refiere el marco regulatorio APEC.

2.3. Puerto Seguro - "Safe Harbor" -USA-

En 1999, Estados Unidos inició negociaciones con la Unión Europea con el objeto de conseguir una declaración de adecuación del nivel de protección de datos personales. Al respecto, se advierte que el problema inicial para el análisis de la protección de datos en los Estados Unidos, se centra en el hecho que en dicho país no existe una normativa sobre protección de datos de carácter personal aplicable en todo el territorio y en todos los sectores de actividad.

Al respecto, se advierte que la Directiva 95/46/CE de la Comisión Europea sobre la protección de datos, a la que nos referiremos en detalle más adelante, prohíbe la transferencia de datos personales a países no pertenecientes a la Unión Europea que no cumplen con el estándar "adecuado" para la protección de la vida privada. Si bien, Estados Unidos y la Unión Europea comparten el objetivo de mejorar la protección de la privacidad de sus ciudadanos, los Estados Unidos tiene un enfoque diferente a la privacidad de los utilizados por la UE.

A fin de salvar estas diferencias de enfoque y proporcionar un medio para que las organizaciones de Estados Unidos puedan cumplir con la Directiva, el Departamento de Comercio de EE.UU., en consulta con la Comisión Europea elaboró un marco de "puerto seguro" para proporcionar la información de una organización haría que evaluar el nivel de protección en materia de datos personales y, de esta manera, vincularse al programa US-EU Safe Harbor.[11]

El Safe Harbor Framework se compone de 7 principios, 15 preguntas más frecuentes[12], las cartas de la Comisión Federal de Comercio, el intercambio de cartas entre el

[11] http://export.gov/safeharbor/eu/index.asp

[12] http://export.gov/safeharbor/eu/eg_main_018474.asp ***Description of the Safe Harbor Frameworks*** Although the respective sets of Safe Harbor Privacy Principles, frequently asked questions and answers (FAQs), and enforcement statements of the two Safe Harbor Frameworks are similar, they differ in a number of ways. Understanding the Safe Harbor Frameworks requires familiarity with all of the relevant documents.

The U.S.-EU Safe Harbor Framework is comprised of 7 Safe Harbor Privacy Principles, 15 FAQs, letters from the Federal Trade Commission and the Department of Transportation on their enforcement powers, the exchange of letters between the U.S. Department of Commerce and the European Commission, and the European Commission's adequacy decision.

The U.S. Department of Commerce holds regular discussions with the European Commission and the Swiss Federal Data Protection and Information Commissioner regarding the administration of the Safe Harbor program. All parties

Departamento de Comercio de EE.UU. y la Comisión Europea , y la decisión de adecuación de la Comisión Europea.

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".

Los principios contenidos en el acuerdo Safe Harbor son los siguientes:

- ✓ **Notice:** Deber de información (o notificación). Las entidades adheridas al Safe Harbor deben informar a los interesados de las finalidades para las cuales han sido recabados sus datos y sobre la forma en que se utilizarán.
- ✓ **Choice:** El principio del consentimiento del afectado. Corresponde al interesado o afectado el poder decidir acerca de la recogida y la transferencia de sus datos de carácter personal a terceros.
- ✓ **Transfers to Third Parties:** Sólo será posible la transferencia de datos cuando las entidades o destinatarios estén suscritos al acuerdo Safe Harbor o sean países miembros de la Unión Europea.
- ✓ **Access:** Las personas deben ser capaces de acceder a la información y corregirla o

concerned emphasize the importance of bilateral cooperation in order to ensure continued data flows and have committed to keep each other informed of any actions that may interrupt data flows.

[13] http://export.gov/safeharbor/en/eg_main_018474.asp Organizations that decide to participate in the Safe Harbor program must comply with one or both of the Safe Harbor Frameworks and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization must reaffirm its self-certification annually to the Department of Commerce, indicating that it continues to adhere to the Safe Harbor program requirements, and of course, it must continue to abide by the Safe Harbor program requirements. It is also required that the organization state in its published privacy policy statement that it adheres to the Safe Harbor Privacy Principles.

eliminarla si no es exacta, a efectos de poder ejercitar los derechos ARCO.

- ✓ **Security:** El principio de seguridad de los datos: Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado".
- ✓ **Data Integrity:** El principio de calidad de los datos. Los datos deben ser fiables y consecuentes con el propósito para el que fueron recopilados.
- ✓ **Enforcement:** Este principio se refiere a la concreta aplicación o ejecución de todo lo que conlleva Safe Harbor. Es un principio controvertido por su ambigüedad, que dispone que para garantizar el cumplimiento de los postulados del Safe Harbor, deben articularse mecanismos independientes de resolución de conflictos y de verificación del cumplimiento de los principios Safe Harbor, con potestad para sancionar, en su caso.

2.4 Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana

La Red Iberoamericana de Protección de Datos (RIPD), nació como consecuencia de un acuerdo logrado entre catorce países en el Encuentro Iberoamericana de Protección de Datos celebrado en el mes de junio del año 2003 en La Antigua, Guatemala.

Las Directrices para la armonización de la Protección de Datos en la Comunidad Iberoamericana, reconocen que en la mayoría de los países de Iberoamérica se consagra el derecho al habeas data como un derecho fundamental e independiente frente al derecho a la intimidad. Pero a la vez, dichas directrices tienen por propósito lograr que este derecho, en muchos países reconocido a nivel constitucional, sea complementado con el establecimiento de un marco normativo uniforme y homogéneo que permita garantizar en Iberoamérica un nivel equivalente de protección, por medio del reconocimiento de normativo de los principios, derechos y deberes que lo configuran.

De esta manera, las directrices que se explicarán a continuación, están encaminadas a delimitar las características y aspectos esenciales del derecho fundamental al habeas data, para así orientar a los estados Iberoamericanos en el desarrollo de sus iniciativas normativas, logrando que se establezca un marco homogéneo de protección que facilite el intercambio de información entre ellos y hacia otros Estados que han adoptado estándares equivalentes o similares de protección.

Los principios, derechos y obligaciones propuestos por las directrices se aplicarían a todo tipo de tratamiento de datos llevado a cabo tanto por entidades del sector público como del privado que no sean realizados con fines exclusivamente relacionados con la vida privada o familiar.

las directrices señalan cinco principios básicos:

- ✓ Tratamiento leal y lícito que consiste en que los datos sólo puedan ser recolectados y tratados de buena fe, con observancia de las disposiciones legales y las Directrices, respetando los derechos de las personas;
- ✓ La limitación de la finalidad que consiste en que los datos sólo puedan ser recolectados y tratados para el cumplimiento de las legítimas finalidades que se determinaron de manera explícita y que estén relacionadas con la actividad de la persona que realiza el tratamiento;
- ✓ Proporcionalidad consistente en que sólo se pueda someter a tratamiento aquellos datos adecuados, pertinentes y no excesivos en relación con las finalidades previstas;
- ✓ Exactitud que se refiere a que los datos se mantengan exactos, completos y actualizados;
- ✓ Conservación que hace referencia a que los datos se cancelen o se conviertan en anónimos cuando hayan dejado de ser necesarios para las finalidades que se previeron.

Se establece además el concepto de "legitimación para el tratamiento" que consiste en que los datos sólo puedan ser recabados o tratados cuando se ha obtenido el consentimiento del interesado, a menos que la ley nacional establezca excepciones razonables y legítimas atendiendo las circunstancias particulares de cada caso, como por ejemplo cuando el tratamiento se realice por parte de la Administración en el ejercicio de sus potestades.

En seguida de la legitimación para el tratamiento, las directrices traen a colación la transparencia e información al interesado que consiste en el deber que tiene quien realiza el tratamiento de datos, de informar al interesado en el momento en el que haga el recabo de los datos, la identidad del responsable, los fines para los cuales los datos vayan a ser tratados, y el modo en que podrá a ser efectivos sus derechos.

Se establecen los derechos del interesado, dentro de los que se encuentran los derechos de acceso, rectificación, cancelación, oposición al tratamiento, indemnización por daños

sufridos como consecuencia de un tratamiento de datos que haya contrariado las directrices, entre otros.

También el texto de las directrices reconoce la importancia de los principios de seguridad y confidencialidad en el tratamiento. El primero consiste en que se adopten todas las medidas necesarias para proteger los datos contra la adulteración, pérdida, acceso no autorizado o uso fraudulento. Y el segundo de ellos, se refiere a que todas las personas que intervengan en cualquier fase del tratamiento de los datos, estarán obligadas a respetar el carácter reservado por principio de esa información, obligación que subsistirá aun después de finalizada su relación con el titular de los datos.

En materia de transferencia internacional de datos, directriz establece ciertas limitaciones. La regla general es que sólo podrán efectuarse transferencias internacionales de datos a aquellos Estados que tengan una legislación que recoja lo dispuesto en las Directrices.

En efecto, de conformidad con lo previsto en el apartado 8 de las directrices:

> "8.2. No obstante la Ley podrá establecer supuestos en que, excepcionalmente, sea posible la transferencia internacional de datos a otros Estados, atendiendo a las circunstancias que concurran en cada supuesto. En todo caso, deberán tenerse en cuenta los derechos e intereses del afectado y, en particular, si el mismo ha prestado su consentimiento a la transferencia en cuestión. (...)
>
> "8.3. Fuera de los supuestos mencionados en los dos párrafos anteriores, sólo será posible la transferencia internacional de datos en caso de que se obtenga la autorización de la autoridad a la que se refiere el apartado 9, para lo cual será necesaria la aportación por parte del exportador de garantías suficiente para asegurar que el importador cumplirá en todo caso lo dispuesto en estas directrices"[14].

En materia de autoridades encargadas del *enforcement*, se establece que aquellas deberán ser independientes e imparciales y contar como mínimo con las siguientes competencias: Conocer de reclamaciones en cuanto al ejercicio de los derechos establecidos en las Directrices; realizar averiguaciones e investigaciones; adoptar medidas para evitar la persistencia en el incumplimiento de las Directrices; mantener un registro de

[14] http://inicio.ifai.org.mx/Estudios/Directrices_de_armonizacion.pdf

los tratamientos llevados a cabo al que puedan acceder los interesados; autorizar transferencias internacionales de datos a Estados cuya legislación no recoja lo dispuesto en las Directrices; promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos; dictaminar proyectos de disposiciones normativas; entre otras.

Finalmente, las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana se refieren al tema de sanciones por violación a la mismas[15] estableciendo que de conformidad con la legislación interna de cada Estado, se impondrán las sanciones correspondientes que podrán ser competencia o bien de las autoridades de protección de datos, o bien de las autoridades judiciales. Sin embargo, se establece que en el caso de que la competencia sancionatoria la tenga la autoridad judicial, entonces la autoridad de protección de datos deberá tener la capacidad suficiente para recurrir a la vía judicial y solicitar que se adopten las medidas necesarias para garantizar el cumplimiento de las Directrices.

3. RECOPILACIÓN DE NORMAS INTERNACIONALES RELACIONADAS CON TRANSFERENCIAS INTERNACIONALES

A continuación procedemos a realizar un recuento de los desarrollos jurídicos y documentos emitidos por organizaciones internacionales en materia transferencia internacional de datos que contienen principios y reglas generales que condicionan la circulación transfronteriza de información personal.

3.1 Organización e las Naciones Unidas (ONU)

La Organización de las Naciones Unidas emitió en 1990 la Resolución 45/95 que contiene una lista básica de principios para la protección de datos personales de aplicación mundial, como el de exactitud de los mismos, la determinación de su finalidad, su acceso y la no discriminación. Los procedimientos para llevar a la práctica las normas relativas a los archivos de datos personales informatizados se dejan a la iniciativa de cada Estado, con sujeción a las siguientes orientaciones:

[15] Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana. "Sanciones 10.1. El incumplimiento de las disposiciones que reflejen lo previsto en estas directrices deberá ser sancionado conforme a la legislación interna. La capacidad para la imposición de las correspondientes sanciones podrá corresponder a la autoridad de protección de datos, a la que se refiere el apartado 9 o a los órganos judiciales."

a) **Principios Relativos a las Garantías Mínimas que deben Prever las Legislaciones Nacionales**

i) Principio de la licitud y lealtad La información relativa a las personas no se deben recolectar ni tratar con procedimientos desleales o ilícitos, ni utilizarse con fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.

ii) Principio de exactitud Las personas encargadas de la creación de un fichero o de su funcionamiento deben tener la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que resultan completos y veraces a fin de evitar los errores por omisión y de que se actualizan periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando.

iii) Principio de finalidad La finalidad de un fichero y su utilización en función de esta finalidad deberían especificarse y justificarse y, en el momento de su creación, ser objeto de una medida de publicidad o en todo caso se deben poner en conocimiento de la persona interesada a fin de que ulteriormente sea posible asegurarse de que: a) Todos los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida; b) Ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado; c) El período de conservación de los datos personales no excede del necesario para alcanzar la finalidad con que se han registrado.

iv) Principio de acceso de la persona interesada Toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne, a conseguir una comunicación inteligible de ella sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando esta información sea comunicada, a conocer los destinatarios. Debería preverse una vía de recurso, en su caso, ante la autoridad encargada del control de conformidad con el principio 8 infra. En caso de rectificación, el costo debería sufragarlo el responsable del fichero. Es conveniente que las disposiciones de este principio se apliquen a todas las personas, cualquiera que sea su nacionalidad o su residencia.

v) Principio de no discriminación A reserva de las excepciones previstas con criterio limitativo en el principio, no deberían registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, sobre la participación en una asociación o la afiliación a un sindicato.

vi) Facultad de establecer excepciones Sólo pueden autorizarse excepciones a los principios 1 a 4 si son necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, en particular, los derechos y libertades de los demás, especialmente de personas perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente por la ley o por una reglamentación equivalente, adoptada de conformidad con el sistema jurídico nacional, en que se definan expresamente los límites y se establezcan las garantías apropiadas. Las excepciones al principio de no discriminación, , deben estar sujetas a las mismas garantías que las previstas para las excepciones a los principios de licitud, exactitud, finalidad, y acceso y sólo podrán autorizarse dentro de los límites previstos por la Carta Internacional de Derechos Humanos y demás instrumentos pertinentes en materia de protección de los derechos y de lucha contra la discriminación.

vii) Principio de seguridad Se deben adoptar medidas apropiadas para proteger los ficheros contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático.

viii) Control y sanciones Cada legislación debe designar a la autoridad que, de conformidad con el sistema jurídico interno, se encarga de controlar el respeto de los principios anteriormente enunciados. Dicha autoridad deberá ofrecer garantías de imparcialidad, de independencia con respecto a las personas u organismos responsables del procesamiento de los datos o de su aplicación, y de competencia técnica. En caso de violación de las disposiciones de la legislación interna promulgada en virtud de los principios anteriormente enunciados, deben preverse sanciones penales y de otro tipo así como recursos individuales apropiados.

ix) Flujo de datos a través de las fronteras Cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos. Cuando no haya garantías comparables, no se podrán imponer limitaciones injustificadas a dicha circulación, y sólo en la medida en que así lo exija la protección de la vida privada.

Tal como lo establece el numeral 10 de la Resolución 45/95 los citados principios deben aplicarse en primer lugar a todos los ficheros computadorizados, tanto públicos como privados y, por extensión facultativa y a reserva de las adaptaciones pertinentes, a los

ficheros manuales. Podrían tomarse disposiciones particulares, igualmente facultativas, para extender la aplicación total o parcial de estos principios a los ficheros de las personas jurídicas, en particular cuando contengan en parte información sobre personas física.

Adicionalmente la Resolución 45/95, establece la denominada **"Cláusula humanitaria"** de conformidad con la cual: "debería preverse de manera específica una excepción a estos principios cuando el fichero tenga por finalidad proteger los derechos humanos y las libertades fundamentales de la persona de que se trate, o prestar asistencia humanitaria. La legislación nacional debería contener una excepción análoga para las organizaciones internacionales gubernamentales en cuyo convenio sobre la sede no se hubiera excluido la aplicación de dicha legislación nacional, así como para las organizaciones internacionales no gubernamentales a que sea aplicable dicha legislación."

La cláusula humanitaria establece la posibilidad de que las organizaciones no gubernamentales se acojan a una excepción de estos principios cuando la finalidad de sus archivos sea la protección de los derechos humanos y las libertades fundamentales de las personas afectadas o la ayuda humanitaria.

El Principio de no discriminación, establece que salvo las excepciones previstas en el Punto 6, que se refieren a la facultad de establecer excepciones, no se podrán recoger datos sensibles que pudieran dar origen a una discriminación ilegal o arbitraria. En el evento de establecer excepciones en relación con este principio, las mismas "soló podrán autorizarse dentro de los límites establecidos en la Carta Internacional de Derechos Humanos y en el resto de instrumentos aplicables en el campo de la protección de los derechos humanos y la prevención de la discriminación".

3.2 Consejo de Europa – Convenio 108

En 1981, el Consejo de Europa adoptó el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, también conocido como "Convenio de Estrasburgo" o "Convenio 108"[16]. El convenio contiene disposiciones aplicables al tratamiento automatizado de datos personales relativos a personas físicas tanto por el sector público como por el privado. No obstante esta condición, debe tenerse

[16] Convenio No 108 del Consejo, de 28 de enero de 1981, de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

en cuenta que en todo caso un país parte podría también aplicar sus disposiciones a los datos concernientes a personas jurídicas y al tratamiento manual de los datos. En efecto, tal como lo dispone expresamente el literal b) del artículo 3 del Convenio 108 el mismo se aplicará "a informaciones relativas agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica."

Resulta pertinente frente a este modelo traer a colación precisamente la reciente regulación colombiana. En Colombia el régimen de protección de datos contenido en la Ley 1581 de 2012 resulta aplicable a datos o información de personas naturales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada[17]. Tal como lo ha precisado la Corte Constitucional, en nuestro país si bien resultan susceptibles de protección los datos e informaciones de las personas jurídicas, la garantía del habeas data para estos entes no es una protección autónoma, "sino una protección que surge en virtud de las personas naturales que las conforman. Por tanto, a juicio de la Sala, es legítima la referencia a las personas naturales, lo que no obsta para que, eventualmente, la protección se extienda a las personas jurídicas cuando se afecten los derechos de las personas que la conforman."[18]

Respecto del flujo transfronterizo de datos personales el convenio requiere una "protección equivalente" entre los países partes, y provee mecanismos de asistencia recíproca y cooperación internacional a través de las autoridades locales de cada país.

Así, el artículo 1 del Convenio 108 del Consejo de Europa de 28 de enero de 1981 establece:

> "El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»).

Por su parte, el artículo 12 del citado convenio establece que:

[17] Ley 1581 de 2012, artículo 2.
[18] Corte Constitucional, Sentencia C- 748 de 2011.

"Flujos transfronterizos de datos de carácter personal y el derecho interno

1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.

2. Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte.

3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2:

a). En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados e datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente;

b). Cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo." (Resaltado fuera del texto)

Se observa que el Convenio 108 del Consejo de Europa sobre la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal, brindó protección explícita a este tipo de información y fijó las pautas del modelo común para dicha protección. El Convenio amplió el catálogo de garantías con la introducción de los principios de lealtad, exactitud, finalidad, pertinencia, utilización no abusiva, olvido, publicidad, acceso individual y seguridad, y con la prohibición de tratamiento automático de datos, que hoy denominamos datos sensibles, esto es aquellos que revelen el origen racial de las personas, sus opiniones políticas, convicciones religiosas o de otro tipo, así como datos sobre su salud o vida sexual

3.2 Directiva 95 N° 95/46/CE del Parlamento Europeo

La Directiva 95 N° 95/46/CE del Parlamento Europeo y del Consejo del 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, establece un régimen normativo exhaustivo en la materia tanto para casos de tratamiento realizado manualmente como de forma automatizada[19]. Aplica tanto en el sector público como en el privado.

Las obligaciones y los derechos establecidos en la Directiva 95/46/CE en realidad se presentan como una construcción elaborada a partir de aquellos principios dispuestos en el Convenio No 108 (1981) del Consejo de Europa, que a su vez no difieren sustancialmente de los incluidos en las directrices de la OCDE (1980) y en las directrices de la ONU (1990). La Directiva 95/46/CE constituye el texto de referencia, a escala europea, en materia de protección de datos personales. La directiva crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE).[20]

Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

La Directiva 95/46 consagra dos de las ambiciones más antiguas del proyecto de integración europea: la realización del mercado interior (en este caso, la libre circulación de datos personales) y la protección de los derechos y libertades fundamentales de las personas[21]; para la Directiva resultan igualmente importantes los dos objetivos.

En efecto, desde el punto de vista jurídico, tal y como lo reconoce el primer informe sobre la aplicación de la Directiva sobre Protección de Datos (95/46 CE)[22], "la existencia de la Directiva se basa en el mercado interior. Estaba justificado legislar a nivel comunitario debido a que las diferencias en el modo en que los Estados miembros enfocaban esta cuestión obstaculizaban la libre circulación de datos personales entre los Estados miembros dependiente encargado de la protección de los mencionados datos. Por otra

[19] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm: "La presente Directiva se aplica a los datos tratados por medios automatizados (base de datos informática de clientes, por ejemplo), así como a los datos contenidos en un fichero no automatizado o que vayan a figurar en él (ficheros en papel tradicionales)."
[20] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm
[21] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm
[22] COMISIÓN DE LAS COMUNIDADES EUROPEAS Bruselas, 15.5.2003 COM(2003) 265 final **INFORME DE LA COMISIÓN Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE)**

parte, la Directiva tiene por su naturaleza una repercusión muy amplia. Existen datos sobre cualquier persona y todas las entidades de cualquier sector de la economía son responsables del tratamiento de datos. Por tanto, aunque su justificación jurídica sea bastante específica, su repercusión es muy amplia y su aplicación debe examinarse teniendo en cuenta lo expuesto."

Ahora bien, el artículo 1 de la Directiva 95 establece el objeto de la misma, y señala:

> "Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales."

Respecto del flujo transfronterizo de datos personales, la Directiva 95 se refiere a dos distintos niveles: un "nivel de protección equivalente", en el caso de transferencias entre los países miembros de la Unión Europea; y un "nivel adecuado de protección", en el caso de flujos de datos hacia terceros países, esto es, aquellos que no son miembros de la Unión Europea.

Así, los considerandos 8 y 9 de la Directiva establecen que:

> "(8) Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, **debe ser equivalente en todos los Estados miembros;** que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones;
>
> (9) Considerando que, a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por

> motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad." (Subrayas y negrillas fuera del texto original).

Por su parte, los considerandos 56 y 57 establecen que:

> "(56) Considerando que los flujos transfronterizos de datos personales son necesarios para la desarrollo del comercio internacional; **que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;**
>
> (57) **Considerando, por otra parte, que cuando un país tercero no ofrezca un nivel de protección adecuado** debe prohibirse la transferencia al mismo de datos personales;" (Subrayas y negrillas fuera del texto).

A la luz de lo dispuesto en el numeral 1 del artículo 25 de la Directiva 95, están prohibidas las transferencias de datos personales a terceros países no miembros de la Unión Europea que no garantizan un "nivel adecuado de protección". Esta prohibición cuenta con las excepciones consagradas en el artículo 26. Dice al respecto la norma:

> "No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta."

En relación con las citadas excepciones, el Grupo del Artículo 29 anteriormente mencionado, en el Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo el 24 de julio de 1998, señala que las misma se refieren en su mayoría "a casos en los que los riesgos para el interesado son relativamente escasos o en los que otros intereses (intereses públicos o del propio interesado) prevalecen sobre los derechos de intimidad del interesado. Como excepciones a un principio general, deben interpretarse restrictivamente. Además, los Estados miembros pueden estipular en la legislación nacional que las excepciones no se apliquen en determinados casos. Este puede ser el caso, por ejemplo, cuando sea necesario proteger a grupos de personas especialmente vulnerables, como los trabajadores o los pacientes."[23]

[23] COMISIÓN EUROPEA DIRECCIÓN GENERAL XV Mercado Interior y Servicios Financieros Libre Circulación de la Información, Derecho de Sociedades e Información Financiera Libre Circulación de la Información, protección de datos y sus aspectos internacionales Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales Documento de Trabajo Transferencias de datos personales a terceros países: aplicación

Resulta especialmente relevante el análisis efectuado por el Grupo en relación con el alcance de las referidas excepciones. Lo anterior, teniendo en cuenta que dicho análisis puede aportar elementos de juicio en la interpretación de las excepciones consagradas en el artículo 26 de la Ley 1581 de 2012 en materia de transferencia internacional de datos personales.

Así, tal como lo manifestó el citado Grupo en el Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, "**la primera de estas excepciones** abarca casos en los que el interesado ha dado su consentimiento inequívocamente a la transferencia prevista. Es importante tener en cuenta que el consentimiento, de acuerdo con la definición del artículo 2.h de la Directiva, debe ser libre, específico e informado. El requisito de información es especialmente relevante porque exige que el interesado esté debidamente informado del riesgo concreto que supone el hecho de que sus datos se transfieran a un país que carece de la protección adecuada. Si no se facilita esta información, dicha excepción no será aplicable. Puesto que el consentimiento debe ser inequívoco, cualquier duda sobre su obtención anularía la aplicabilidad de la excepción. Esto podría significar que en muchas situaciones en que el consentimiento se da por sobreentendido (por ejemplo, porque la persona ha sido informada de una transferencia y no se ha opuesto), la excepción no resultaría aplicable. Sin embargo, la excepción será útil cuando el remitente esté en contacto directo con el interesado y sea posible facilitar sin problemas la información necesaria y obtener un consentimiento inequívoco. Normalmente, éste será el caso en transferencias emprendidas en el contexto de, por ejemplo, la suscripción de seguros."

Es importante a este respecto tener en cuenta el examen efectuado por la Corte Constitucional Colombiana mediante sentencia C-748 de 2011 respecto de la excepción consagrada en el literal a) del artículo 26 de la Ley 1581 de 2012 de conformidad con el cual la prohibición de transferencias internacionales de datos no regirá cuando se trate de información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia.

Así, en lo relacionado con la autorización expresa u otorgamiento del consentimiento al

de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998

que se refiere el literal a) del artículo 26 de la citada ley, la Corte concluyó que esta excepción es en desarrollo del principio de la libre voluntad del titular, que está facultado para autorizar la circulación de su información personal. Por lo tanto, es claro que aunque se permite la transferencia de datos a un país que no brinda estándares de protección adecuados, la misma se realiza bajo la responsabilidad de su titular.

De esta manera la Corte Constitucional manifestó que la premisa de contar con la autorización del titular de la información que es objeto de transferencia, es el presupuesto que indudablemente permite la circulación de los datos.

Ahora bien, en relación con las **excepciones segunda y tercera del artículo 26 de la Directiva 95,** el Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, precisó que dichas excepciones "abarcan transferencias necesarias para la ejecución de un contrato entre el interesado y el responsable del tratamiento (o para la ejecución de medidas precontractuales adoptadas a petición del interesado) o para la celebración o ejecución de un contrato celebrado en interés del interesado entre el responsable del tratamiento y un tercero. Aparentemente, estas excepciones son potencialmente bastante amplias, pero, al igual que las excepciones cuarta y quinta comentadas a continuación, es probable que su aplicación en la práctica se vea limitada por la "prueba de necesidad": todos los datos transferidos deben ser necesarios para la ejecución del contrato. Así, si se transfieren datos complementarios que no son esenciales o si el objetivo de la transferencia no es la ejecución del contrato sino otro (mercadotecnia de seguimiento, por ejemplo) se invalidará la excepción. Respecto de las situaciones precontractuales, esta excepción sólo abarca situaciones iniciadas por el interesado (como una solicitud de información sobre un servicio particular) y no las que derivan de propuestas de mercadotecnia planteadas por el responsable del tratamiento.

"A pesar de estas salvedades, las excepciones segunda y tercera tienen bastante peso. Es probable que sean aplicables con frecuencia, por ejemplo, en las transferencias necesarias para reservar un billete de avión de un pasajero, o en transferencias de datos personales necesarios para la transacción de un banco internacional o de un pago con tarjeta de crédito. De hecho, la excepción de contratos "en interés del interesado" (artículo 26.1.c) abarca específicamente la transferencia de datos relativos a los beneficiarios de los pagos bancarios, quienes, aunque sean interesados, es posible que a menudo no sean parte de un contrato celebrado con el responsable del tratamiento que realiza la transferencia."

Las excepciones 2 y 3 de la Directiva 95 se encuentran consagradas en nuestro ordenamiento en el literal e) del artículo 26 de la Ley 1581 que señala que la prohibición de transferencias internacionales de datos no regirá cando se trate de "Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular." Esta, excepción, tal como lo manifestó la Corte Constitucional en sentencia C-748 de 2012 "prevé aquellas transferencias que se realizan teniendo como fundamento una relación de tipo contractual, la cual se regirá bajo lo estipulado en el respectivo contrato y conforme a los deberes y derechos estipulados en cabeza de los extremos contractuales, siendo en esta medida el Responsable del Tratamiento del dato, quien debe velar por el adecuado manejo de la información, sin olvidar que para su transferencia se requiere de la autorización del titular, autorización que, conforme a lo reiteradamente expuesto, se entenderá debe ser previa y expresa."

La cuarta excepción consagrada en el artículo 26 de la Directiva 95 tiene dos vertientes. Al respecto el Documento de Trabajo Transferencias de datos personales a terceros países aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, señala que "la primera engloba las transferencias necesarias o legalmente exigidas por un interés público importante. Este aspecto puede abarcar ciertas transferencias limitadas entre administraciones públicas, aunque hay que tener cuidado de no interpretar esta disposición en sentido muy amplio. Para justificar una transferencia no basta con alegar un interés público, debe ser un interés público importante. El considerando 58 declara que, normalmente, se incluirán los datos transferidos entre administraciones fiscales o aduaneras, o entre servicios competentes en materia de seguridad social. Es posible que también las transferencias entre organismos supervisores de los servicios financieros se beneficien de la excepción. La segunda vertiente se refiere a las transferencias que tienen lugar en el contexto de litigios o procedimientos judiciales internacionales, concretamente transferencias necesarias para el reconocimiento, ejercicio o defensa de derechos legales."

Nuevamente resulta relevante traer a colación la previsión colombiana al respecto. En nuestra legislación esta excepción se encuentra consagrada en el literal f) del artículo 26 de la Ley 1581 de 2012 que establece como excepción a la prohibición general de transferencias internacionales de datos las "transferencias legalmente exigidas para la salvaguarda del interés público, o para el reconocimiento, ejercicio, o defensa de un derecho en un proceso judicial"

Teniendo en cuenta que la citada disposición maneja términos que pueden ser objeto de imprecisiones y que dada su naturaleza amplia y ambigua generan inconvenientes al momento de su aplicación, la Corte Constitucional la declaró inexequible la expresión "*necesarias*" mediante sentencia C-748 de 2011. Al respecto, la citada Corporación manifestó que "las expresiones "*necesarias*" y "*o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial*", no ofrecen suficiente claridad sobre su ámbito de aplicación y si, por el contrario, van en contra de los principios de finalidad, autorización y circulación restringida de los datos personales."

En efecto, señala la Corte que "por una parte, la expresión "*necesarias*" resulta abierta, ambigua y general en el sentido de que no establece respecto de quien se reputa dicha necesidad, ni quien la define, ni cómo se establece. Por otro lado, la expresión "*o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial*" no especifica si el proceso judicial involucra al titular de los datos directamente como encausado o como testigo; en qué calidad y bajo qué circunstancias se hace imperiosa la transmisión, o si, por otro lado, se refiere a los derechos de un tercero. En consecuencia, teniendo en consideración que se trata de la regulación del derecho fundamental al *habeas data*, debe recordarse que las limitaciones impuestas a su ejercicio a través de la consagración de excepciones, han de ser precisas sin emplear conceptos que por su grado de indeterminación pueden comprometer el ejercicio o el goce de otros derechos constitucionales. Se trata de una defensa del principio de legalidad que pretende ofrecer seguridad jurídica a las personas y, en esta medida, conocer con certeza cuándo sería viable la transferencia de datos personales a países que no otorgan garantías de protección adecuados."

Ahora bien, el Documento de Trabajo Transferencias de datos personales a terceros países aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, señala que **la quinta excepción de la Directiva 95** "se refiere a las transferencias necesarias para proteger los intereses vitales del interesado. Un ejemplo evidente sería la transferencia urgente de datos médicos a un tercer país, en el caso de un turista que, habiendo recibido anteriormente tratamiento médico en la UE, haya sufrido un accidente o haya enfermado gravemente. Sin embargo, es preciso tener en cuenta que el considerando 31 de la Directiva interpreta con bastante concreción el "interés vital" como un interés "esencial para la vida del interesado". Esta interpretación normalmente excluye, por ejemplo, los intereses financieros, de propiedades o familiares."

Esta excepción corresponde, bajo la ley colombiana de protección de datos personales, a la salvedad contenida en el literal b) del artículo 26 de la Ley 1581 de 2012, que permite las transferencias internacionales en el evento que se trate de intercambio de datos de carácter médico, cuándo así lo exija el Tratamiento del Titular por razones de salud o higiene pública. Al respecto, la Sentencia C-748 de 2011 de la Corte Constitucional precisó que la excepción se justifica, puesto que en este caso se trata de preservar y garantizar derechos de rango fundamental. Aclara la Corte que la facultad de autorizar la transferencia del dato médico recae no sólo en su titular sino también en sus familiares o representante legal, ya que dicho dato puede ser requerido en circunstancias donde su titular no se encuentre en capacidad de otorgar la autorización.

Finalmente, el Documento de Trabajo Transferencias de datos personales a terceros países aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE señala que "**La excepción sexta y última del artículo 26 de la Directiva 95** se refiere a las transferencias realizadas desde registros que por la ley se han destinado a la consulta pública, si se cumplen las condiciones de consulta en cada caso particular. La intención de esta excepción es que cuando un registro de un Estado miembro esté disponible para consulta pública o por personas que demuestren un interés legítimo, el hecho de que la persona con derecho a consultar el registro se encuentre en un tercer país y que la consulta conlleve el hecho de una transferencia de datos, no impida que se le transmita la información. El considerando 58 especifica que es preciso no permitir la transferencia de la totalidad de los datos o categorías de datos contenidos en el mencionado registro en virtud de esta excepción. Dadas estas restricciones, no hay que considerarla una excepción general relativa a la transferencia de datos de registros públicos. Por ejemplo, es evidente que las transferencias masivas de datos de registros públicos con fines comerciales o la búsqueda de datos a disposición del público con el fin de realizar perfiles de personas físicas específicas no se beneficiarían de la excepción."

Presentadas las excepciones previstas a nivel europeo, vale la pena precisar que la Unión Europea utiliza el estándar de "nivel adecuado de protección" en relación con terceros países. A efectos de establecer la existencia de ese nivel de protección, la Directiva 95 prevé varios criterios que permiten determinar si un país ofrece un nivel de protección adecuado o no. Así, la el artículo 25.2 de Directiva 95 señala que la adecuación "se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en

una categoría de transferencias de datos" e indica los criterios eventualmente aplicables[24]:

> "El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países."

Al adoptar un criterio tan amplio, se requiere un análisis caso a caso para efectos de determinar si un país provee el nivel de protección requerido. De acuerdo con el Grupo, hay dos elementos esenciales que deben verificarse en cualquier análisis relativo al "nivel adecuado de protección": (i) el contenido de las reglas aplicables y (ii) los medios para asegurar su efectiva aplicación. Así, la evaluación requiere constatar la apropiada adopción y cumplimiento de las disposiciones sobre protección de datos personales.

En lo relacionado con el aspecto material, el Grupo interpreta el "nivel adecuado de protección" como correspondiente a un conjunto de disposiciones que garanticen los derechos de los titulares de datos personales, la imposición de obligaciones a los responsables de tratamiento, el establecimiento de principios aplicables al tratamiento de los datos, y la determinación de responsabilidades en caso de infracción.

Para asegurar una efectiva aplicación de las normas, el Grupo identifica el nivel de cumplimiento y la disponibilidad de mecanismos para tal efecto, tales como recursos judiciales y sistema de sanciones. En ese sentido se advierte que la característica principal de la Directiva 95 en este punto es la exigencia de una autoridad independiente que supervisa el cumplimento de la ley.

En efecto, en el "documento de trabajo del Grupo sobre Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea" se establece que la existencia de mecanismos de cumplimiento es indispensable para que un sistema de protección de datos pueda en la

[24] Directiva 94 Artículo 25.2 de la "Directiva de protección de datos".

práctica otorgar un nivel adecuado de protección, dado que supone la existencia de mecanismos de control de los principios contenidos en las leyes nacionales.

Así el citado documento de trabajo establece que tomando la Directiva 95/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, debería ser posible lograr un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento/de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección.

En este contexto, el mencionado documento sugiere incluir en la legislación interna de los Estados miembros los siguientes principios, a los que denomina "de contenido":

1) **Principio de limitación de objetivos** - los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia.

2) **Principio de proporcionalidad y de calidad de los datos** - los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

3) **Principio de transparencia** - debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 11.23 y 13 de la Directiva.

4) **Principio de seguridad** - el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

5) **Derechos de acceso, rectificación y oposición** - el interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos.

6) Restricciones respecto a transferencias sucesivas a otros terceros países - únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la directiva

En relación con los denominados **mecanismos del procedimiento/de aplicación** el documento de trabajo del Grupo sobre Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea señala como condiciones mínimas requeridas:

> 1) Ofrecer un nivel satisfactorio de cumplimiento de las normas. (Ningún sistema puede garantizar el 100 % de cumplimiento, pero algunos son mejores que otros). Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.
>
> 2) Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.
>
> 3) Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

En conclusión, se advierte que la Directiva 95 consagra un "nivel de protección equivalente" entre los países miembros de la Unión Europea, los cuales no pueden obstaculizar el flujo de datos personales dentro del mercado interno. Por su parte, la

directiva exige un "nivel adecuado de protección" a terceros países; en el evento de que un país no cuente con tal nivel, las transferencias están prohibidas.

Ahora bien, es necesario tener en cuenta que la Directiva europea establece una cláusula de homologación con compromisos internacionales, de conformidad con la cual "la Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas."

Finalmente, se advierte que en el año 2001, se expidió un Protocolo Adicional al Convenio, "Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos", el cual ha introducido modificaciones a las disposiciones que reglamentan el flujo transfronterizo de datos personales[25].

3.4 Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Tal como consta en la exposición de motivos de la propuesta de reglamento[26] la iniciativa actualización normativa es el resultado de una amplia consulta de todas las partes

[25] Artículo 1 del Protocolo Adicional: Cada Parte dispondrá que una o más autoridades sean responsables de garantizar el cumplimiento de las medidas previstas por su derecho interno que hacen efectivos los principios enunciados en los Capítulos II y III del Convenio, así como en el presente Protocolo. A este efecto, las autoridades mencionadas dispondrán, en particular, de competencias para la investigación y la intervención, así como de la competencia para implicarse en las actuaciones judiciales o para llamar la atención de las autoridades judiciales competentes respecto de las violaciones de las disposiciones del derecho interno que dan efecto a los principios mencionados en el apartado 1 del artículo 1 del presente Protocolo. Cada autoridad de control atenderá las reclamaciones formuladas por cualquier persona en relación con la protección de sus derechos y libertades fundamentales respecto de los tratamientos de datos de carácter personal dentro de su competencia.

Las autoridades de control ejercerán sus funciones con total independencia. as decisiones de las autoridades de control que den lugar a reclamaciones podrán ser objeto de recurso ante los tribunales.
De conformidad con lo dispuesto en el Capítulo IV, y sin perjuicio de lo dispuesto en el artículo 13 del Convenio, las autoridades de control cooperaran entre sí en la medida

[26] COMISIÓN EUROPEA Bruselas, 25.1.2012 COM(2012) 11 final 2012/0011 (COD)Exposición de motivos Propuesta de **REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que**

interesadas sobre la revisión del actual marco jurídico para la protección de datos de carácter personal, que se prolongó durante más de dos años e incluyó una conferencia de alto nivel celebrada en mayo de 2009 y dos fases de consulta pública. Los objetivos de la expedición del reglamento comprenden el impacto de las nuevas tecnologías de la información y las comunicaciones y la necesidad de minimizar las diferencias entre las legislaciones de los distintos países europeos.

En efecto, se ha reconocido que si bien los principios incorporados desde la Directiva siguen siendo válidos, la evolución de las telecomunicaciones y las opciones de transmisión de datos y bases informáticas de manera cada vez más amplia, rápida y hasta cierto punto imperceptible (desarrollo de bases de datos en la nube), junto con el acelerado crecimiento del comercio internacional imponen contar con reglas claras, homogéneas, sencillas, hasta cierto punto competitivas que permitan a los países de la Unión Europea conciliar la necesidad de protección de los derechos de los ciudadanos con la realidad de la globalización[27].

Los objetivos de la expedición del reglamento comprenden tanto el impacto de las nuevas tecnologías de la información y las comunicaciones como la necesidad de minimizar las diferencias entre las legislaciones de los distintos países europeos.

La Comisión Europea estableció que su propuesta se basaría en un reglamento y no en una directiva como la existente actualmente -Directiva 95/46/CE- en la medida en que se ha considerado al reglamento como un instrumento más idóneo para alcanzar los objetivos de armonización[28]. En cuanto al objeto de la propuesta, éste no difiere en lo esencial de lo que establece la actual Directiva. Se trata, tal como se acaba de mencionar,

respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)

[27] Ver, COMISIÓN EUROPEA Bruselas, 25.1.2012 COM(2012) 11 final 2012/0011 (COD) Exposición de motivos de la Propuesta de **REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)**

[28] COMISIÓN EUROPEA Bruselas, 25.1.2012 COM(2012) 11 final 2012/0011 (COD) Propuesta de **REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) numeral 3.2.** "Se considera que un Reglamento es el instrumento jurídico más apropiado para definir el marco de la protección de datos personales en la Unión. La aplicabilidad directa de un reglamento, de conformidad con el artículo 288 del TFUE, reducirá la fragmentación jurídica y ofrecerá una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento del mercado interior."

de proteger los derechos y libertades fundamentales de las personas y, en particular, su derecho a la privacidad cuando se tratan sus datos personales y, al mismo tiempo, garantizar la libre circulación de dichos datos personales dentro de las fronteras de la Unión Europea.

Dentro de la exposición de motivos de la propuesta de reglamento se señala que si bien el marco jurídico actual vigente en la Unión Europea es adecuado y completo en cuanto a sus principios y objetivos, la manera de aplicarse en la Unión es fragmentada.

Así, la exposición de motivos de la propuesta de reglamento señala:

> "Ha llegado por ello el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas".

Con el objetivo de solucionar la dificultades derivadas de la fragmentación en la aplicación del marco regulatorio actual, se propone este Reglamento, teniendo como fundamento el artículo 288 del Tratado de Funcionamiento de la Unión Europea (en adelante TFUE), que señala que un reglamento es un instrumento jurídico que tiene aplicabilidad directa en todos los países miembros.

En efecto, el fundamento jurídico que sustenta la Propuesta de Reglamento recae en el artículo 16 del TFUE, según lo señala expresamente la citada exposición de motivos:

> "La presente propuesta se basa en el artículo 16 del TFUE que constituye la nueva base jurídica para la adopción de las normas de protección de datos introducida por el Tratado de Lisboa. Esta disposición permite la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión. También permite la adopción de normas relativas a la

libre circulación de datos de carácter personal, incluidos los datos personales tratados por los Estados miembros u operadores privados"[29].

En cuanto al articulado general de la propuesta de Reglamento, se pueden ver importantes cambios y modificaciones a la actual Directiva 95/46/CE en algunos aspectos importantes.

El artículo 4 propuesto contiene definiciones de los términos utilizados en la Directiva. Si bien algunas definiciones se mantienen, otras se modifican, o son complementadas con elementos adicionales. Algunas se introducen por vez primera («violación de los datos personales», «datos genéticos»; «datos biométricos»; «datos relativos a la salud»; «establecimiento principal»; «representante»; «empresa»; «grupo de empresas»; «normas corporativas vinculantes»; «niño» (basada en la Convención de las Naciones Unidas sobre los derechos del Niño), y «autoridad de control».[30]

Por otro lado, en el artículo 5 donde se establecen los principios del tratamiento de datos personales, se puede ver que corresponden a los establecidos en la Directiva 95/46/CE pero se introducen nuevos elementos como el principio de transparencia y el establecimiento de una responsabilidad general del responsable del tratamiento.

En cuanto a las obligaciones en cabeza del responsable, se añade la obligación de informar a los interesados el período de conservación de los datos, así como los derechos de rectificación, supresión e interposición de reclamaciones que les asisten. De igual manera se profundiza en otras obligaciones como por ejemplo en la de suministrar información al interesado, haciéndola extensiva incluso sobre el período de conservación de los datos. Así mismo, se extiende la obligación de seguridad al encargado del tratamiento, independientemente del contrato suscrito que tenga con el responsable. Por último vale la pena resaltar con respecto a las obligaciones del los que recolectan y procesan datos personales la obligación que se introduce consistente en realizar una evaluación de impacto de la protección de datos de manera previa a realizar operaciones de tratamiento arriesgadas.

[29] Propuesta de Reglamento General de Protección de datos. Bruselas, 2012. Encontrado en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF
[30] Propuesta de **REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) numeral 3.4**

En lo que tienen que ver con los derechos de los titulares, se establece el derecho al olvido estableciendo cuáles son sus condiciones, dentro de las cuales se encuentra la obligación del responsable que haya difundido los datos personales de informar a los terceros sobre la solicitud de supresión. Así mismo, se introduce el derecho a la portabilidad de los datos que consiste en poder transferir los datos de un tratamiento electrónico a otro sin que el responsable lo pueda impedir.

En materia de transferencia internacional de datos, en el artículo 40 se establece, como principio general, que la observancia de las exigencias que establece dicho capítulo es de obligado cumplimiento para toda transferencia de datos de carácter personal a terceros países u organizaciones internacionales.

El artículo 41 fija los criterios, condiciones y procedimientos para la adopción de una decisión relativa a la adecuación del nivel de protección de datos por parte de la Comisión, basada en el artículo 25 de la Directiva 95/46/CE. Entre los criterios que deberán tenerse en cuenta para que la Comisión evalúe si existe o no un nivel adecuado de protección se incluyen expresamente el Estado de Derecho, el recurso jurisdiccional y la supervisión independiente.[31]

Adicionalmente el artículo 41 consagra expresamente la posibilidad de que la Comisión evalúe el nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país. Para las transferencias a terceros países en relación con las cuales la Comisión no haya adoptado ninguna decisión de adecuación, el artículo 42 requiere que se aporten las garantías apropiadas, especialmente cláusulas tipo de protección de datos, normas corporativas vinculantes y cláusulas contractuales. La posibilidad de hacer uso de cláusulas tipo de protección de datos de la Comisión se basa en el artículo 26, apartado 4, de la Directiva 95/46/CE.[32]

El artículo 44 define y aclara las excepciones a una transferencia de datos sobre la base de las disposiciones en vigor del artículo 26 de la Directiva 95/46/CE. Ello se aplica en particular a las transferencias de datos requeridas y necesarias para la protección de intereses públicos importantes, por ejemplo en caso de transferencias internacionales de datos entre autoridades de competencia, administraciones fiscales o aduaneras, o entre

[31] Ibidem 3.4.5. CAPÍTULO V – TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES
[32] Ibidem 3.4.5. CAPÍTULO V – TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

servicios competentes en materia de seguridad social o de gestión de la pesca. Por otra parte, en determinadas circunstancias una transferencia de datos puede estar justificada por un interés legítimo del responsable o del encargado del tratamiento, aunque únicamente después de haber evaluado y documentado las circunstancias de dicha operación de transferencia.[33]

El artículo 45 establece explícitamente mecanismos de cooperación internacional para la protección de los datos de carácter personal entre la Comisión y las autoridades de control de terceros países, especialmente aquellas que se considera que ofrecen un nivel de protección adecuado, teniendo en cuenta la Recomendación de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la cooperación transfronteriza en la ejecución de leyes que protegen la privacidad, de 12 de junio de 2007.[34]

En lo que se refiere a la autoridad de control, se atribuye una nueva competencia a la autoridad principal en caso de que un responsable o encargado del tratamiento se encuentre establecido en varios Estados Miembros, logrando así una aplicación uniforme. "El artículo 52 establece las funciones que ha de desempeñar la autoridad de control, entre las que se incluye conocer e investigar las reclamaciones y fomentar el conocimiento de los ciudadanos en materia de riesgos, normas, garantías y derechos. El artículo 53 dispone los poderes de la autoridad de control, basado en parte en el artículo 28, apartado 3, de la Directiva 95/46/CE y en el artículo 47 del Reglamento (CE) no 45/2001, y añadiendo algunos elementos nuevos, incluido el poder de sancionar infracciones administrativas". [35]

La Sección Tercera de la Propuesta del Reglamento instituye el Consejo Europeo de Protección de Datos que sustituirá al Grupo de Protección de las Personas creado en el artículo 29 de la Directiva 95/46/CE. Se establecen las funciones de este nuevo órgano y su forma de organización y decisión.

En materia de recursos judiciales, responsabilidad y sanciones, también se introducen ciertas modificaciones a la Directiva 95/46 encaminadas a lograr una mayor aplicabilidad

[33] Ibidem numeral 3.4.5. CAPÍTULO V – TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES
[34] Ibidem numeral 3.4.5. CAPÍTULO V – TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES
[35] Propuesta de Reglamento General de Protección de datos. Bruselas, 2012. Encontrado en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

de la protección de datos personales y de dotar a los interesados de instrumentos útiles y efectivos para obtener la protección de sus derechos.

Se puede concluir de la exposición de motivos de la Propuesta de Reglamento y de la totalidad del articulado, que la propuesta parte de los fundamento de la Directiva 95/46 y amplía algunos aspectos. Con el Reglamento se logra una mayor protección y efectividad del derecho de habeas data, buscando una mayor homogeneidad en la aplicación de la normatividad en todos los países de la Unión Europea y respondiendo a las necesidades que han surgido en la práctica.

4. CASOS PRÁCTICOS RELACIONADOS CON ACEPTACIÓN DE TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

A continuación presentamos una síntesis de algunos casos importantes en los que diferentes autoridades internacionales han tenido la oportunidad de evaluar si ciertos países cuentan con un nivel adecuado de protección de datos que haga posible una transferencia de datos a ellos, y ha establecido así si cuentan con unos estándares mínimos de protección:

4.1. Dictamen del Grupo de Protección de Datos Personales de Europa en lo que respecta al Tratamiento de Datos Personales en Argentina:

En esta oportunidad, el Grupo de Protección de Datos Personales de Europa[36] estudió la legislación argentina bajo las reglas de la Directiva 45/96/CE para determinar si contenía unos estándares equivalentes que permitieran concluir que en dicho país se contaba con un nivel adecuado de protección.

En este estudio, se determinó que la legislación argentina cuenta con los principios básicos en materia de protección de datos como son el principio de limitación de objetivos, el principio de proporcionalidad y calidad de datos, el principio de transparencia y el principio de seguridad así como con los derechos de acceso, rectificación y oposición que están también establecidos en la citada directiva europea. De igual manera, se pudo concluir en este estudio, que la legislación argentina cuenta con mecanismos de procedimiento y aplicación efectivos para garantizar los derechos del titular de la información, así como con unas sanciones efectivas y disuasorias.

[36] El Grupo de Trabajo, creado por el artículo 29 de la Directiva 95/46/CE, es un órgano consultivo independiente de la U Esobre protección de datos y vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

En este Dictamen de octubre de 2002, el Grupo de Trabajo concluyó que:

"Argentina garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el apartado 6 del artículo 25 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. Sin embargo, el Grupo de Trabajo invita también a las autoridades argentinas a tomar las medidas necesarias para solucionar los puntos débiles de los actuales instrumentos legales identificados en el presente dictamen y solicita a la Comisión Europea continuar el diálogo con el Gobierno argentino con el citado objetivo. En particular, el Grupo de Trabajo insta a las autoridades argentinas a garantizar la aplicación efectiva de la legislación a nivel provincial mediante la creación de los necesarios órganos de control independientes en los casos en los que éstos no existan y, mientras tanto, a buscar soluciones temporales apropiadas que sean conformes con el orden constitucional argentino"[37].

Es importante recordar que los criterios y requisitos establecidos por Grupo de Protección de Datos Personales de Europa, a efectos de determinar la existencia de un nivel adecuado de protección de datos, se encuentran contenidos en el Documento de Trabajo sobre Transferencias de datos personales a terceros países y aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, aprobado por el Grupo de Trabajo el 24 de julio de 1998. Tal como se señala en el mencionado documento, los objetivos de un sistema de protección de datos, y los estándares de calidad que debe ofrecer la legislación de un Estado para ser considerado como adecuado, son:

- ✓ Asegurar un nivel satisfactorio de cumplimiento de las normas.
- ✓ Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos.
- ✓ Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

La presencia de estos elementos fue verificada satisfactoriamente en la legislación Argentina, (tanto en la leyes de carácter general como en los reglamentos expedidos en materia de protección de datos). Eso llevó a que el Grupo de Protección de Datos Personales de Europa, concluyera que dicho país garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el apartado 6 del artículo 25 de la Directiva

[37] GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS. Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina. Bruselas, 3 de octubre de 2002.

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.

4.2 Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46 del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act

En este caso, la Comisión estudió el contenido de la ley canadiense de protección de datos personales que se aplica a las entidades privadas que recogen, utilizan o divulgan datos personales en sus actividades comerciales. El Personal Information and Electronic Documents Act (en adelante "la Ley canadiense") de 13 de abril de 2000 aplica a las entidades privadas que recojan, utilicen o divulguen datos personales en sus actividades comerciales. La mencionada ley, tiene el carácter de federal, pero se establece que las provincias deberán adoptar legislaciones similares de conformidad con los principios y estándares mínimos contenidos en dicha ley federal.

Con el propósito de establecer el nivel adecuado de protección exigido por la Unión Europea, la Comisión consideró todos los elementos relativos a la aplicación y entrada en vigencia de la ley canadiense. En este sentido, y a partir de la información suministrada por Canadá, la Comisión estableció que se previeron distintas etapas para la aplicación de la ley a los sujetos que realizan actividades de tratamiento de datos personales en dicho país.

En el análisis se evidenció que a partir del 1 de enero de 2001, la ley canadiense aplicó a todos los datos personales, excluidos los de carácter sanitario, que las entidades que operen como "empresa federal" recojan, utilicen o divulguen en el transcurso de sus actividades económicas. Dichas empresas operan en sectores como el transporte aéreo, la banca, la radiotelevisión, el transporte interprovincial y las telecomunicaciones. También se aplicará a todos las entidades que comercian con datos personales fuera de su provincia o fuera del Canadá y a los datos laborales sobre los asalariados de las empresas federales.[38]

[38] Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46 del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act

A partir del 1 de enero de 2004, la ley amplió su aplicación a cualquier organismo que recoja, utilice o divulgue datos personales en el transcurso de una actividad comercial dentro de una provincia, independientemente de que dicho organismo esté o no regulado a escala federal.

No obstante la cobertura de la ley, la comisión advirtió que no están sujetas a la ley canadiense las entidades a quienes se aplique la Federal Privacy Act o se regulen por el sector público de ámbito provincial. Del mismo modo, las actividades filantrópicas o sin fines lucrativos tampoco están sujetas a la Ley canadiense a no ser que tengan carácter comercial. No se aplica, por último, a los datos laborales utilizados con fines no comerciales siempre que no se refieran a los asalariados del sector privado sujeto a regulación federal. En tales casos, la autoridad canadiense de protección de la vida privada podrá proporcionar información adicional.[39]

A fin de que se respete el derecho de las provincias a legislar en su ámbito competencial, la comisión verificó que la ley federal establece que cuando éstas adopten una legislación similar, las entidades y ámbitos de organización y actividad que dicha legislación cubra estarán exentos de la Ley federal. El apartado 2 del artículo 26 de la Personal Information Protection and Electronic Documents Act faculta al Gobierno federal para, "si tiene el convencimiento de que una Ley provincial esencialmente similar a la presente parte se aplica a una organización -o categoría de entidades-o a una actividad -o categoría de actividades-, excluir la organización, actividad o categoría de la aplicación de la presente parte en lo relativo a la recogida, utilización o comunicación de datos personales realizadas en el interior de la provincia".

El Governor in Council (Gobierno federal canadiense) concede por decreto las excepciones a la legislación que sea básicamente similar. (Order-in-Council). Siempre que una provincia adopte una legislación básicamente similar, las entidades y ámbitos de organización y actividad que cubra estarán exentos de aplicar la Ley federal en transacciones en el interior de la provincia. La Ley federal seguirá aplicándose a toda recolección, utilización o divulgación de datos interprovincial e internacional, así como en todos aquellos casos en que las provincias no hayan creado una legislación que sea básicamente similar ni total ni parcialmente las excepciones a la legislación que sea básicamente similar.

[39] Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46 del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act

Finalmente la Comisión tuvo en cuenta que Canadá se adhirió formalmente el 29 de junio de 1984 a las Orientaciones de la OCDE sobre la protección de la vida privada y los flujos de datos transfronterizos de 1980.[40]

De acuerdo con lo anterior, es claro que la Ley canadiense comprende todos los principios fundamentales necesarios para que las personas físicas reciban una protección adecuada. La aplicación de estas normas se garantiza mediante recursos jurisdiccionales y el control independiente que ejercen autoridades como el Comisario federal de protección de la vida privada, dotado de facultades de investigación e intervención. Además, las disposiciones de derecho canadiense relativas a la responsabilidad civil se aplican en caso de tratamiento ilícito que haya causado daños.

4.3. Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza

En esta oportunidad, la Comisión estudió la ley federal suiza de protección de datos, de junio de 1992, cuya aplicación se ha determinado mediante diferentes decretos federales. Adicional a la ley federal, se estudiaron ciertas normas cantonales que regulan la protección de datos personales en ciertas materias como por ejemplo en hospitales públicos.

Del estudio mencionado, la Comisión concluyó que "Las normas de Derecho aplicables en Suiza incluyen todos los principios esenciales necesarios para constatar la existencia de un nivel de protección adecuado de la protección de las personas físicas, aunque también se prevén excepciones y limitaciones para la salvaguarda de intereses públicos importantes. La aplicación de estas normas está garantizada mediante recursos jurisdiccionales y el control independiente que ejercen autoridades como el "*Préposé fédéral à la protection des données et à la transparence*", dotado de facultades de investigación e intervención. Además, las disposiciones de Derecho suizo relativas a la responsabilidad civil se aplican en caso de tratamiento ilícito que haya causado daños". [41]

No obstante lo anterior, la Comisión dispuso en esta oportunidad que a pesar de comprobarse un nivel adecuado de protección de datos, por motivos de transparencia se

[40] Ibidem
[41] Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza

especificarían algunas circunstancias excepcionales que podrían dar lugar a la suspensión de flujos específicos de información.

Así, se estableció que sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con disposiciones diferentes del artículo 25 de la Directiva 95/46/CE, las autoridades correspondientes de los Estados miembros podrían ejercer su facultad de suspender los flujos de datos hacia un receptor en Suiza para proteger a los particulares contra el tratamiento de sus datos personales, en los siguientes casos:

a) La autoridad suiza competente resuelve que el receptor vulnera las normas de protección correspondientes; o

b) Existen razones para creer que la autoridad suiza competente no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados; y las autoridades competentes del Estado miembro han hecho esfuerzos razonables en estas circunstancias para notificárselo al responsable del tratamiento establecido en Suiza y proporcionarle la oportunidad de alegar.

4.4. Decisión de la Comisión de 21 de noviembre de 2003 relativa al carácter adecuado de la protección de los datos personales en Guernsey

En este caso, la Comisión estudió la ley de 2001 vigente en Guernsey sobre protección de datos junto con los demás instrumentos legislativos que con el mismo propósito se han adoptado desde esa fecha.

En Guernsey, las normas relativas a la protección de datos personales basadas en los preceptos de la Directiva 95/46/CE se recogen en la referida ley de 2001 o Data Protection (Bailiwick of Guernsey) Law que entró en vigor el 1 de agosto de 2002. Asimismo, en 2002 se han adoptado en Guernsey 16 instrumentos legislativos (decretos), en los que se establecen normas específicas sobre cuestiones como el acceso de los titulares de los datos, el tratamiento de los datos sensibles y la notificación a la autoridad de protección de datos. Estos instrumentos son un complemento de la Ley. La Comisión consideró que Guernesey ofrecía un nivel adecuado de protección de datos, teniendo en cuenta que:

"Las normas de Derecho aplicables en Guernsey cubren todos los principios básicos necesarios para ofrecer un nivel adecuado de protección a las personas físicas. La aplicación de estas normas está garantizada mediante recursos jurisdiccionales y el control independiente que ejercen autoridades como el Comisario de protección de datos, dotado de facultades de investigación e intervención".

4.5. Decisión de la Comisión de 28 de abril de 2004 relativa al carácter adecuado de la protección de los datos personales en la Isla de Man

En esta oportunidad, la Comisión estudió la ley de la Isla de Man bajo los principios de la Directiva 95/46).

En la Isla de Man la protección de datos está regulada por la Data Protection Act 2002 (Ley de protección de datos de 2002). Desde el 1 de abril de 2003, dicha Ley deroga y sustituye a la Data Protection Act de 1986. Aunque la isla de Man no pertenece a la UE y, por tanto, no está obligada a respetar lo dispuesto en la Directiva europea de protección de datos (Directiva 95/46/CE), ha adoptado medidas para ello a fin de solicitar una resolución de conformidad de la Comisión Europea. La ley de 2002 incluye normas similares a las del estatuto de protección de datos de 1998 de Inglaterra y Gales. Su título completo es An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information («Ley relativa a la nueva normativa para regular el tratamiento de la información sobre las personas, incluida la obtención, conservación, utilización y comunicación de dicha información»).

El Grupo de Trabajo señala que la evaluación del carácter adecuado de la legislación sobre protección de datos vigente en la Isla de Man hace referencia esencialmente a la Ley de protección de datos de 2002. El citado Grupo comparó los preceptos de dicha Ley con las principales disposiciones de la Directiva, teniendo en cuenta el dictamen del Grupo de Trabajo sobre «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE». Este dictamen, como se ha venido reiterando a lo largo del presente documento enuncia una serie de principios que constituyen un «núcleo» de principios de «contenido» de protección de datos y de requisitos de «procedimiento/de aplicación», cuyo cumplimiento es un requisito mínimo para juzgar adecuada la protección.

Teniendo en cuenta lo anterior, el Grupo de Protección de Datos Personales de Europa considera que la Isla de Man garantiza un nivel de protección adecuado según lo dispuesto en el apartado 6 del artículo 25 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.

5. ESTÁNDARES ADECUADOS DE PROTECCIÓN CONFORME LA LEGISLACIÓN Y JURISPRUDENCIA COLOMBIANAS

Con fundamento en los criterios establecidos por la Corte Constitucional mediante sentencia C- 742 de 2011, que se ocupó de examinar la constitucionalidad de la Ley 1581 de 2012, relacionados con el nivel adecuado de protección de datos, y a los cuales hicimos referencia en la parte primera del presente documento, hemos elaborado una tabla que contiene cada uno de tales criterios, e incluye la legislación de cada país, que permitirá determinar, cuáles países cuentan con un nivel adecuado de protección de datos personales y cuáles no, de conformidad con lo establecido por la Corte Constitucional, y la Ley 1581 de 2012.

Es importante tener en cuenta que los criterios establecidos por la Corte Constitucional, se desprenden directamente de los parámetros fijados por el Grupo del artículo 29 sobre Protección de Datos de la Unión Europea, contenidos principalmente en el Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998.

De acuerdo con lo señalado en el artículo 26 de la Ley 1581 de 2012, el principio general que rige en las transferencias internacionales a un país que no tenga un «*nivel de protección adecuado* » es la concurrencia de cualquiera de las excepciones previstas en la misma norma. En los demás casos, deberá comprobarse la existencia de ese nivel adecuado con fundamento en los estándares fijados por la Superintendencia de Industria y Comercio.

Así, para efectos de facilitar a la Superintendencia de Industria y Comercio la identificación y desarrollo de tales estándares, procedemos a proponer los criterios que pueden ser tenidos en cuenta por la entidad para efectos de establecer el nivel adecuado de protección en el marco de una transferencia internacional de datos. Tales criterios han sido elaborados con base en lo establecido por la Corte Constitucional y en especial en el Documento de Trabajo Transferencias de datos personales a terceros países:

aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998.

Así, los estándares de protección que, a la luz de lo establecido en el artículo 26 de la Ley 1581 de 2012, debe ofrecer la legislación de un Estado para ser considerados como adecuados deben ser examinados desde dos puntos de vista: (i) el contenido de las normas aplicables a los datos personales y (ii) los mecanismos procesales existentes establecidos para garantizar la eficacia de dichas normas.

Tomando como base el Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998, procedemos enumerar aquellos principios que constituyen principios de "contenido" de protección de datos y de requisitos "de procedimiento/de aplicación", cuyo cumplimiento es un requisito indispensable para estimar adecuada la protección.

(i) Principios de contenido: se diferencian dos tipos de principios de contenido, los *básicos* y los *adicionales* aplicables a tipos específicos de tratamiento.

a) Principios básicos:

- ✓ **Limitación de objetivos**: los datos deben tratarse con una finalidad específica y posteriormente utilizarse o transferirse únicamente en cuanto no sea incompatible con la finalidad de la transferencia
- ✓ **Proporcionalidad y calidad de los datos**: los datos deben ser exactos y, cuando sea necesario, estar actualizados, así como adecuados, pertinentes y no excesivos con relación la finalidad para la que se transfieren o traten posteriormente. Transparencia: debe informarse a los interesados acerca de la finalidad del tratamiento y de la identidad del responsable del tratamiento en el país tercero, y de cualquier otro elemento necesario para garantizar un tratamiento legítimo
- ✓ **Seguridad:** el responsable debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presente el tratamiento; toda persona que actúe bajo su autoridad, incluido el encargado, no debe tratar los datos salvo bajo sus instrucciones.
- ✓ **Derechos de acceso, rectificación y oposición**: el interesado debe tener derecho a obtener una copia de todos sus datos y a rectificar los inexactos.

b) Principios adicionales

- ✓ **Datos sensibles**: cuando se trate de datos sensibles la legislación deberá contemplar mecanismos de protección reforzada.
- ✓ **Datos de niños, niñas y** adolecentes la legislación revisada deberá prever instrumentos específicos de protección para el tratamiento de información de menores de edad.

(ii) Mecanismos de procedimiento/aplicación:

Un modelo adecuado de protección de datos personales debe proporcionar tanto un nivel satisfactorio de cumplimiento de las normas como asistencia a los titulares de la información en el ejercicio de sus derechos, así como instrumentos y mecanismos apropiados de recurso para quienes que resulten perjudicados en el caso de que no se observen las normas. Así, se entenderá que la legislación de un país cumple con un nivel adecuado de protección cuando:

- ✓ Asegura un nivel satisfactorio de cumplimiento de las normas.
- ✓ Ofrece apoyo y asistencia a los interesados en el ejercicio de sus derechos.
- ✓ Ofrece vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

6. TABLA LEGISLACIÓN COMPARADA-CRITERIOS ESTABLECIDOS POR LA CORTE CONSTITUCIONAL

País (Norma)	Obligaciones de las partes	Derechos del titular	Principios sobre los datos (Calidad del dato y seguridad jurídica)	Procedimiento de protección de datos (Mecanismos y Autoridades)
Colombia (Ley 1581 de 2012	En el artículo 12 se consagra para el responsable del tratamiento el deber de informar al titular sobre el tratamiento que se le dará a los datos; los derechos que le asisten; el carácter facultativo de sus respuestas sobre datos sensibles; y su identificación y teléfono. Adicionalmente, en el Título VI se consagran los deberes para los responsables y encargados del tratamiento.	En el artículo 8 se consagran los derechos del titular entre los que están: conocer, actualizar y rectificar sus datos; solicitar prueba de la autorización; ser informado respecto del uso que se le ha dado a sus datos; presentar quejas ante la autoridad competente; revocar la autorización y solicitar la supresión del dato.	En el artículo 4 se establecen los principios para el tratamiento de datos personales dentro de los que se encuentra el principio de seguridad de acuerdo con el cual cada responsable o encargado del tratamiento debe manejar la información con medidas técnicas, humanas y administrativas necesarias para evitar su adulteración, pérdida, y acceso no autorizado. A su vez, se establece el principio de veracidad o calidad en virtud de cual, la información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada comprobable y comprensible. El Decreto Reglamentario de la ley establece en su Título VIII las medidas de seguridad en el tratamiento de datos.	El Título V consagra todos los procedimientos de protección de datos. El artículo 14 establece el trámite de las consultas; el artículo 15 establece los reclamos; el artículo 19 establece quién es la autoridad de protección de datos; el artículo 22 y siguientes, establecen el trámite para las sanciones, los montos, límites y efectos de las mismas, y los criterios para su graduación.
España (Ley 15 de 1999 y Real Decreto 1720 de 2007 por el cual "se aprueba el Reglamento de desarrollo de la Ley Orgánica")	El artículo 1 de la Ley 15 de 1999 establece para el responsable del tratamiento el deber de secreto sobre los datos. No se encuentra la existencia de un título especial que consagre los deberes u obligaciones de los responsables. Sin embargo, en el decreto reglamentario, en el artículo 20 se establecen las relaciones entre el responsable y el encargado, asignándole a cada uno de ellos unos deberes específicos; el artículo 52 consagra unas obligaciones previas al tratamiento de los datos.	El artículo 5 establece el derecho de los titulares a ser informados de manera previa a la obtención de los datos acerca de la finalidad del tratamiento, del carácter obligatorio o facultativo de sus respuestas, de sus derechos de acceso, rectificación, cancelación y oposición, y de la identidad y dirección del responsable del tratamiento. El artículo 3 establece los derechos de las personas.	El artículo 4 establece la calidad de los datos personales que se pueden recoger para su tratamiento. El artículo 9 establece lo concerniente a la seguridad de los datos. El artículo 39 establece el Registro General de Protección de Datos.	El artículo 35 establece la autoridad nacional de protección de datos; el artículo 45 establece los tipos de sanciones que se pueden imponer; y el artículo 48 establece el procedimiento sancionador. El Decreto Reglamentario de la ley 15 de 1999, establece en su Título IX los procedimientos tramitados ante la autoridad nacional de protección de datos.
México Ley Federal de Protección de datos personales en posesión de los particulares de 2010.	El artículo 6 de la ley establece los principios de licitud, consentimiento de información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad que deberán ser observados por los responsables del tratamiento. El artículo 14 de la ley establece que el responsable del tratamiento deberá velar por el cumplimiento de los principios de protección de datos personales establecidos en la ley, debiendo adoptar todas las medidas necesarias para su aplicación; el artículo 15 dispone que el responsable tiene la obligación de informar a los titulares, acerca de la información que se recaba de ellos y con qué fines a través de un aviso de privacidad.	El Capítulo III de la ley establece los derechos de los titulares de datos personales, entre los que están el derecho de acceso, rectificación, cancelación y oposición; y el Capítulo IV de la ley regula el ejercicio de dichos derechos.	El artículo 38 de del Reglamento, establece los procedimientos para conservación, bloqueo, y supresión de datos personales. Los artículos 59 y siguientes lo establecen lo relativo a las funciones de seguridad, los factores para determinar las medidas de seguridad, y las acciones para la seguridad de los datos. Dentro de los principios establecido en el artículo 6 de la ley, se encuentra el principio de calidad de los datos.	El Capítulo VI de la ley, establece las autoridades en materia de protección de datos; el Capítulo VII establece el procedimiento para la protección de datos personales; el Capítulo IX establece el procedimiento de imposición sanciones; el Capítulo X establece las infracciones y sanciones a la ley; y el Capítulo XI establece los delitos en materia del tratamiento indebido de datos personales.
Argentina (Ley 25.326 y Normas Complementarias y Reglamentarias).	No hay un capítulo o artículo específico que establezca las obligaciones y deberes de los responsables del tratamiento. Sin embargo, en diferentes apartes de la ley se establecen algunos de sus deberes y responsabilidades.	El Capítulo III de la ley establece los derechos de los titulares de datos dentro de los que están el derecho de información, el derecho de acceso, el derecho de rectificación, actualización o supresión y el derecho a la impugnación.	El artículo 4 de la ley establece la calidad de los datos personales. El artículo 9 de la ley establece la seguridad de los datos. El artículo 21 de la ley establece el registro de archivos de datos.	El artículo 29 establece el órgano de control y sus funciones. Los artículos 31 y 32 de la ley establecen las sanciones administrativas y penales a las que da lugar la violación de las disposiciones de la ley. El Capítulo VII de la ley regula la acción de protección de datos personales.
Paraguay (Ley 1682 de 2001"Reglamenta la Información de Carácter Privado").	No hay un capítulo o artículo específico que establezca las obligaciones y deberes de los responsables del tratamiento.	No hay un capítulo o artículo específico que establezca los derechos de los titulares de datos.	No se ve de manera explícita el principio de seguridad ni la definición de la calidad de los datos.	No se establece una autoridad de control especializada en la protección de datos personales. El artículo 10 de la ley establece los casos en los que las autoridades competentes aplicarán sanciones.
Chile (Miembro del APEC) (Ley 19.628 de 1999)	No hay un capítulo o artículo específico que establezca las obligaciones de los	El Título II establece los derechos de los titulares de datos	No se ve de manera explícita el principio de seguridad ni la	El artículo 16 establece el procedimiento de acuerdo con el cual

	responsables de manera directa.	personales dentro de los que se encuentran el derecho de información, modificación, cancelación y bloqueo.	definición de la calidad de los datos.	el titular tendrá derecho a recurrir ante un juez cuando considere vulnerados sus derechos. El Título V establece la responsabilidad por las infracciones a la ley.
Brasil (Ley 9.507 de 1997)	No hay un artículo o capítulo que se refiera específicamente a las obligaciones de los responsables del tratamiento de datos personales.	El artículo 7 define el habeas data como el derecho a conocer las informaciones relativas a las personas que consten en bancos de datos, y el derecho a rectificar los datos y el derecho de hacer anotaciones.	No hay un artículo que consenga el principio de seguridad na de calidad de los datos personales.	El artículo 20 establece las autoridades competentes en materia de habeas data.
Nicaragua (Ley 787 de 2012)	El artículo 7 de la ley establece la obligación para los responsables del tratamiento de informar al titular de los datos de manera previa a la recolección de los mismos, la finalidad, la existencia del fichero, el carácter obligatorio o facultativo de sus respuestas, entre otros aspectos. El artículo 11 establece como deber para el responsable, adoptar medidas de seguridad; el artículo 12 establece el deber de confidencialidad El artículo 22	El Capítulo III establece los derechos del titular de los datos personales.	El artículo 11 establece las medidas de seguridad que debe adoptar el responsable del tratamiento. El artículo 18 establece los requisitos de la información estableciendo entre otros, que debe ser clara y sencilla. El artículo 30 regula el registro de ficheros de datos.	El Capítulo V crea y regula las funciones de la autoridad de control de datos personales, llamada Dirección de Protección de Datos Personales. El Capítulo VI establece las infracciones y sanciones a la ley. El Capítulo VII establece las acciones de protección de datos personales.

	establece la obligatoriedad de inscripción en el registro de ficheros de datos. El artículo 33 establece las obligaciones frente a los requerimientos del inspector.			
Perú (Ley 29733 de 2011)	El Título IV establece las obligaciones del titular y del encargado del banco de datos personales dentro de los cuales se encuentran efectuar el tratamiento una vez obtenido previo consentimiento informado, expreso e inequívoco; no recopilar datos por medios fraudulentos; actualizar los datos, almacenar los datos de manera tal que se posibilite el ejercicio de los derechos del titular; suprimir los datos que hayan de ser necesarios para la finalidad para la cual fueron recopilados; entre otros.	El Título III establece los derechos del titular de datos personales dentro de los cuales se encuentran el derecho de información, el derecho de acceso, el derecho de actualización, inclusión, rectificación y supresión, el derecho a impedir el suministro, el derecho de oposición, el derecho al tratamiento objetivo, el derecho de tutela y el derecho a ser indemnizado.	El artículo 8 establece el principio de calidad de los datos, estableciendo que deben ser veraces y exactos. El artículo 9 establece el principio de seguridad, de acuerdo con el cual el titular de los datos y el encargado de su tratamiento deben adoptar todas las medidas necesarias para garantizar la seguridad de los datos personales.	El Título VI establece la Autoridad Nacional de Protección de Datos Personales y sus funciones. El Título VII regula lo concerniente a las infracciones a la ley y las sanciones administrativas.
Guatemala (Decreto 57-2008)	En el Capítulo Sexto se establecen los deberes de los responsables del tratamiento de datos, dentro de los que se encuentran, adoptar los procedimientos adecuados para recibir y responder las solicitudes de	No hay un capítulo o artículo que regule y enumere los derechos del titular de datos.	No hay un artículo específico que establezca de manera expresa, la calidad y seguridad de los datos personales.	El Título II establece el procedimiento de acceso a la información pública. El Título V establece lo concerniente a las sanciones.

	acceso y corrección; administrar los datos sólo cuando sean adecuados y pertinentes en relación con los propósitos para los cuales fueron obtenidos; adoptar todas las medidas necesarias que garanticen la seguridad y reserva de los datos.			
Bolivia	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección da datos personales. El derecho está consagrado en la constitución así "Art. 130. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar y obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, que afecten su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección de datos personales.

		reputación, podrá interponer la Acción de Protección de Privacidad".		
Ecuador	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección de datos personales. Sin embargo, el artículo 92 de la Constitución Política consagra la Acción de Habeas Data de acuerdo con la cual toda persona tiene derecho a conocer de la existencia y a acceder a los documentos o bancos de datos personales que consten en entidades públicas o privadas, así como a conocer su uso, finalidad, origen y destino. Así mismo, se consagra en este artículo el derecho a la rectificación, eliminación o anulación.	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección de datos personales. En el artículo 92 de la constitución se establece expresamente que no existe un órgano de control respecto de los temas de habeas data, sino que en dichos casos se acudirá a las acciones judiciales.
Venezuela	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección de datos personales.
Costa Rica (Ley 8968 de 2011) "Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales"	El artículo 5 consagra la obligación de informar de modo expreso, preciso e inequívoco, de manera previa a la solicitud de los datos personales por	El artículo 7 establece los derechos que le asisten a toda persona, consistentes en el acceso a la información y a la rectificación.	El artículo 6 establece el principio de calidad de la información de acuerdo con el cual los datos recolectados deben ser actuales,	Los artículos 15 y 16 establecen la creación de la Agencia de Protección de datos de los Habitantes (Prodhab) y sus atribuciones.

Valbuena ABOGADOS

	parte de quien los pretenda recopilar. El artículo 10 establece el deber de seguridad; el artículo 11 establece el deber de confidencialidad.	El artículo 13 establece el derecho de toda persona a un procedimiento administrativo sencillo y rápido para la protección de los derechos contenidos en la ley.	veraces, exactos y adecuados al fin para el cual fueron recolectados. El artículo 10 establece el principio de seguridad de los datos de acuerdo con el cual el responsable deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos y evitar su alteración, destrucción, pérdida y acceso no autorizado.	El Capítulo V regula lo relativo a los procedimientos en materia de protección de datos personales.
El Salvador- Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas	Únicamente existe una regulación de carácter sectorial la **Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas.** La Ley está dirigida a aquellas personas jurídicas o privadas que tengan autorización para operar como agencias de información de datos y agentes económicos que mantengan o manejen datos sobre el historial de crédito de los consumidores con el objeto de proteger el derecho constitucional a la Intimidad.	Únicamente existe una regulación de carácter sectorial la **Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas.** La Ley está dirigida a aquellas personas jurídicas o privadas que tengan autorización para operar como agencias de información de datos y agentes económicos que mantengan o manejen datos sobre el historial de crédito de los consumidores con	Únicamente existe una regulación de carácter sectorial la **Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas.** La Ley está dirigida a aquellas personas jurídicas o privadas que tengan autorización para operar como agencias de información de datos y agentes económicos que mantengan o manejen datos sobre el historial de crédito de los consumidores con el objeto de proteger el derecho	Únicamente existe una regulación de carácter sectorial la **Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas.** La Ley está dirigida a aquellas personas jurídicas o privadas que tengan autorización para operar como agencias de información de datos y agentes económicos que mantengan o manejen datos sobre el historial de crédito de los consumidores con el objeto de proteger el derecho constitucional a la Intimidad.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

		el objeto de proteger el derecho constitucional a la Intimidad.	constitucional a la Intimidad.	
Panamá Ley 6 del 22 de enero de 2002	No existe una ley general en materia de protección de datos personales. Existe sólo una ley en materia de transparencia para la gestión pública (Ley 6 de 2002) y otra ley en materia de servicio de información sobre historial crediticio (Ley 24 de 2002).	No existe una ley general en materia de protección de datos personales. Existe sólo una ley en materia de transparencia para la gestión pública (Ley 6 de 2002) y otra ley en materia de servicio de información sobre historial crediticio (Ley 24 de 2002).	No existe una ley general en materia de protección de datos personales. Existe sólo una ley en materia de transparencia para la gestión pública (Ley 6 de 2002) y otra ley en materia de servicio de información sobre historial crediticio (Ley 24 de 2002).	No existe una ley general en materia de protección de datos personales. Existe sólo una ley en materia de transparencia para la gestión pública (Ley 6 de 2002) y otra ley en materia de servicio de información sobre historial crediticio (Ley 24 de 2002).
Honduras	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección de datos personales.	No existe una ley general en materia de protección de datos personales.
Estados Unidos ("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	Se establece el rol de las autoridades de protección de datos, y cómo las organizaciones que administren datos, deben cooperar con ellas.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

			los propósitos para los cuales se va a usar.	
Australia	No existe una ley que regule la protección de datos de manera general. Existe el "Freedom Information Act" de 1982 que sólo aplica para las bases de datos de carácter público.	No existe una ley que regule la protección de datos de manera general. Existe el "Freedom Information Act" de 1982 que sólo aplica para las bases de datos de carácter público.	No existe una ley que regule la protección de datos de manera general. Existe el "Freedom Information Act" de 1982 que sólo aplica para las bases de datos de carácter público.	No existe una ley que regule la protección de datos de manera general. Existe el "Freedom Information Act" de 1982 que sólo aplica para las bases de datos de carácter público.
Canadá Personal Information and Eectronic Documents Act del 13 de abril de 2000.	No se establecen de manera clara, las obligaciones de los responsables del tratamiento. Sin embargo, con base en el "Personal Information Protection and Electronic Document Act", se han expedido diferentes directrices y guías como el "Privacy and Online Behavioural Advertising" que determina los principios mínimos que deben contener los códigos internos de cada empresa, dentro de los cuales se encuentran las obligaciones y deberes de los responsables, como la obtención del consentimiento del titular, el establecimiento de medidas que garanticen la seguridad y protección de los datos, etc.	No se establecen de manera clara, las obligaciones de los responsables del tratamiento. Sin embargo, con base en el "Personal Information Protection and Electronic Document Act", se expidió el "Código Modelo para la Protecc ión de Datos Personales de la Asociación Canadiense de Estándares" en el que se establece el principio de acceso el cual consiste en el derecho que tiene el titular de datos para acceder a las bases de datos que contengan información personal suya y conocer cuál es el uso que se le dará, así como el derecho a solicitar su modificación, eliminación.	No se establece el principio de seguridad y calidad de los datos; Sin embargo, con base en el "Personal Information Protection and Electronic Document Act", se expidió el "Código Modelo para la Protección de Datos Personales de la Asociación Canadiense de Estándares" en el que sí se establecen de manera clara los principios de seguridad y calidad del dato. Cabe anotar, que las organizaciones no tienen obligatoriamente que adoptar este Código, sino que de acuerdo con sus necesidades y características adoptarán un código similar.	Se establece como autoridad en materia de protección de datos personales el Comisionado para la Privacidad. Personal Information Protection and Electronic Document Act", está basado fundamentalmente en el establecimiento de sanciones e investigaciones en cabeza del Comisionado para la Privacidad, que se inician a partir de las visitas que realiza dicho Comisionado.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

China	No cuenta todavía con una legislación nacional obligatoria en materia de protección de datos personales. No obstante, existe una Guía titulada "Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems", que contiene algunos parámetros que deberán ser tenidos en cuenta en las legislaciones sectoriales.	No cuenta todavía con una legislación nacional obligatoria en materia de protección de datos personales. No obstante, existe una Guía titulada "Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems", que contiene algunos parámetros que deberán ser tenidos en cuenta en las legislaciones sectoriales.	No cuenta todavía con una legislación nacional obligatoria en materia de protección de datos personales. No obstante, existe una Guía titulada "Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems", que contiene algunos parámetros que deberán ser tenidos en cuenta en las legislaciones sectoriales.	No cuenta todavía con una legislación nacional obligatoria en materia de protección de datos personales. No obstante, existe una Guía titulada "Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems", que contiene algunos parámetros que deberán ser tenidos en cuenta en las legislaciones sectoriales.
Indonesia	No existe una legislación consolidada en materia de protección de datos personales.	No existe una legislación consolidada en materia de protección de datos personales.	No existe una legislación consolidada en materia de protección de datos personales.	No existe una legislación consolidada en materia de protección de datos personales.
Japón ***Personal Information Protection Law (Act) y Law Summary from Jonesday Publishing***	Se establecen las obligaciones para quien recoja información personal en sus bases de datos dentro de las cuales está especificar el propósito de uso de la información; no variar el propósito sin el consentimiento del titular; revelar su identificación personal y los	Se establecen los derechos del titular dentro de los cuales se encuentran el acceso a la información, el derecho a corregirla o solicitar su eliminación en determinados casos, entre otros.	Se establece el principio de seguridad y calidad de los datos.	Se establece una autoridad en materia de protección de datos personales y las sanciones que pueden imponer por violación a las normas establecidas.

	procedimentos para que el titular pueda acceder a su información; entre otras.			
Corea *Act on Personal Information Protection of Public Agencies y Act on Information and Communication Network Usage*	El artículo 15 establece los deberes y obligaciones de quien recolecta información personal, dentro de los cuales se encuentran obtener el consentimiento del titular; informar sobre el propósito que deberá cumplir el uso que se haga de esa información; informar el término durante el cual se usará la información recolectada; tomar las medidas conducentes para impedir que la información sea alterada o dañada; entre otros.	El artículo 4 establece los derechos del titular dentro de los cuales se encuentra el derecho a ser informado en relación con el procesamiento de su información; el derecho a dar el consentimiento, o a negarlo en relación con el uso de sus datos; el derecho a corregir o solicitar la destrucción de su información; entre otros. Adicionalmente, el Capítulo V desarrolla de manera detallada los derechos del titular garantizando su efectividad.	El artículo 29 establece el principio de seguridad. A pesar de que no hay un artículo que establezca de forma expresa el principio de calidad o veracidad de la información personal, de todo el "Personal Information Protection Act", se puede concluir que esta principio se encuentra garantizado.	El Capítulo II establece una autoridad en materia de protección de datos personales llamada "Personal Information Protection Commission" y las sanciones que se pueden imponer, con sus respectivos procedimientos.
Malasia *Common Law principle of confidentiality; Draft Personal data Protection Bill y Banking and Financial Institutions Act of 1989 privacy provisions*	Se establecen obligaciones y deberes para el usuario de la información dentro de los cuales se encuentran la obtención del consentimiento del titular; la adopción de medidas conducentes a proteger la información de destrucción, acceso indebido y otras eventualidades; la	Se establece el derecho de los titulares de acceder a su información y de solicitar su corrección o eliminación.	Se establece el principio de seguridad y el principio de integridad de la información que es equivalente al principio de calidad o veracidad.	Se establece una autoridad en materia de protección de datos, y las sanciones que puede imponer con la descripción de los procedimientos respectivos.

	no divulgación de la información a terceras personas sin el consentimiento del titular; adoptar procedimientos que le permitan a los titulares el acceso a su información, entre otros.			
Nueva Zelanda ("Privacy Act 1993")	Se establece en el primer principio, el deber para las agencias que recolecten información, de establecer el propósito para el cual efectúan la recolección. En el principio número dos, se establece el deber de recolectar la información de forma directa del titular de la información y no de un tercero. En el tercer principio se establece el deber de informar al titular de la información acerca de la identificación de quien recolecta la información.	Los principios seis y siete, establecen en cabeza de los titulares de la información, los derechos de acceso y corrección de sus datos.	El principio número cinco establece el principio de seguridad de la información. En el principio número ocho se establece el principio de calidad de la información.	Se establece en la Sección 13, una autoridad en materia de protección de datos personales y sus funciones. En caso de violaciones al Privacy Act, la autoridad deberá llevar el caso ante un Tribunal para que imponga las sanciones respectivas.
Nueva Guinea Filipinas	No existe una ley que regule la protección de datos de manera general.	No existe una ley que regule la protección de datos de manera general.	No existe una ley que regule la protección de datos de manera general.	No existe una ley que regule la protección de datos de manera general.
Rusia ley Personal Data No. 152-FZ July 2006	La ley prevé las obligaciones para el operador de la información personal, dentro de las cuales se encuentran: obtener un consentimiento previo por parte del titular; procesar la información de	La ley establece dentro de los derechos de los titulares de datos personales, el derecho al acceso, modificación y eliminación de la información así como el derecho	Se establece el principio de seguridad de la información. No se encuentra de forma expresa el principio de veracidad o claridad de los datos. No obstante,	Se establece una autoridad de regulación nacional y las sanciones que puede imponer con sus respectivos procedimientos.

	acuerdo con las leyes rusas; informar al titular acerca de la información de quien recolecta la información; entre otras.	a impedir la transferencia de sus datos a terceros. Adicionalmente se establece el derecho a obtener una compensación cuando se le causen daños por el mal uso de su información.	de la totalidad de la ley, se puede concluir que se tienen las medidas adecuadas para lograr que los datos sean precisos, conformes a la realidad, y claros.	
Singapur ("Personal Data Protection Act")	No hay una sección o capítulo que establezca de manera expresa las obligaciones y deberes de los controladores o responsables de la información. No obstante lo anterior, la Sección IV establece el requisito para quien va a procesar información personal, la obtención del consentimiento del titular, y las características del mismo. Así mismo, la División 2 de la Sección Primera, limita el procesamiento de datos al propósito para el cual fueron recolectados y hasta un término determinado de conformidad con el propósito. De igual manera, se establece en cabeza de quien procesa la información, el deber de informarle	La Sección V del "Personal Data Protection Act" establece los derechos de acceso a la información y corrección de los datos personales en cabeza del titular de la información.	La Sección VI del "Personal Data Protection Act" establece el principio de calidad o veracidad de la información así como el principio de seguridad.	La Sección II del "Personal Data Protection Act" establece la autoridad de control en materia de protección de datos personales y sus funciones. La Sección X regula los procedimientos de investigación, y las sanciones a imponer en caso de violaciones a la ley.

	al titular la finalidad para la cual se están recolectando los datos personales.			

País (Normas)	Obligaciones de las partes	Derechos del titular	Principios sobre la(s) datos (Calidad del dato y seguridad técnica)	Procedimiento de protección de datos (Mecanismos y Autoridades)
Miembros de la Unión Europea				
Alemania **Federal Data Protection Act (BDSG) 2009**	la Parte I establece las normas generales dentro de las cuales está: 1) el principio de legalidad (sección 4) que incluye la obligación de obtener el consentimiento del titular, de notificar a la autoridad competente sobre el procesamiento de datos, entre otras; y 2) la obligación de confidencialidad (sección 5). Por último, las secciones 7 y 8 establecen el deber de compensar al titular por daños causados con el tratamiento de los datos.	La sección 6 establece como inalienables del titular de los datos: 1) el derecho de acceso (regulado en las secciones 19 y 34); 2) el derecho de rectificación, supresión o bloqueo (secciones 20 y 35)	Las secciones 9 y 9a (así como el anexo a la norma) obligan a quienes manejan datos personales a tomar las medidas técnicas y de seguridad necesarias para verificar el cumplimiento de la ley.	La sección 21 así como el capítulo 3 (secciones 22 a 26) regulan lo concerniente a la autoridad encargada de verificar el cumplimiento de la Ley. Esta autoridad es el Federal Commissioner for Data Protection and Freedom of Information. En la parte V de las provisiones finales se establecen faltas administrativas y penales para quienes incumplan la ley (secciones 43 y 44)
Austria **Federal Act Concerning the Protection of Personal Data (DSG 2000)**	La sección 6 establece entre los principios generales el de legalidad, manejo justo de los datos, y el de finalidad. También consagra obligaciones para los responsables del tratamiento de los datos. La sección 11 establece las	Las secciones 26 y siguientes establecen los derechos del titular de los datos así: - Sección 26: derecho de acceso a la información - Sección 27: derecho de rectificación y supresión - Sección 28: derecho de objeción	La sección 6 establece las condiciones de calidad de los datos. La sección 14 establece las normas sobre la seguridad de los datos	Las secciones 29 y siguientes establecen los procedimientos legales para asegurar la eficacia de la Ley y enumeran las funciones de la Data Protection Commission, hoy denominada Austrian data protection authority y del Data

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

	obligaciones del encargado del tratamiento de datos. La sección 15 establece el principio de confidencialidad en el tratamiento de los datos La sección 17 establece el deber del responsable del tratamiento de datos, de notificar a la autoridad competente antes de iniciar su procesamiento. La sección 24 establece el deber del responsable del tratamiento de informar al titular sobre la recolección de datos personales			Protection Council (secciones 35 a 44) Finalmente las secciones 31, 32 y 33 establecen un procedimiento administrativo y uno judicial para que los titulares puedan denunciar el incumplimiento de la ley y obtener la compensación correspondiente. Las secciones 51 y 52 consagran sanciones penales y administrativas ante el incumplimiento de la Ley.
Belgica Loi relative à la protection de la vie privée à l'egard des traitements de donnees à caractere personnel (loi vie privée) 1992 Modificada por: La Ley del 11 de diciembre de 1998 y la Ley del 26 de febrero de 2003	El artículo 4 establece los principios de legalidad y finalidad en el tratamiento de los datos. El artículo 5 establece las condiciones para el manejo de datos personales, dentro de las que se cuenta la obligación de obtener el consentimiento del titular. El artículo 9 establece el deber de información al titular sobre la obtención de sus	El artículo 2 establece que toda persona tiene derecho a la protección de sus libertades y derechos fundamentales, particularmente el derecho a la privacidad. El artículo 10 consagra el derecho de acceso a los datos por parte del titular. El artículo 12 consagra el derecho de exigir la rectificación, supresión o	El artículo 4, además de los principios generales de legalidad y finalidad, establece las condiciones bajo las cuales de asegura la calidad de los datos personales. Establece que los datos personales deben ser adecuados, pertinentes y no excesivos en relación con las finalidades para las que fueron obtenidos. Afirma que deben ser exactos y actualizados. Por último, deben ser conservados durante un tiempo necesario para el desarrollo de su finalidad.	Los artículos 13 y 14 consagran la posibilidad del titular de los datos personales de acudir a la autoridad competente (Commission de la protection de la vie privée) o a los tribunales para exigir la protección de sus derechos. Los artículo 23 a 36 establecen la conformación y funciones de la Commission de la protection de la vie privée. Encargada de vigilar el cumplimiento de la

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

	datos personales	prohibición de utilización de la información incorrecta, inexacta o desactualizada.	El artículo 16 establece la obligación de quienes manejen los datos personales de adoptar las medidas técnicas y organizacionales necesarias para asegurar el adecuado manejo de los datos.	Ley. Los artículos 37 a 43 establecen sanciones ante el incumplimiento de la Ley
Bulgaria Personal Data Protection Act 2002 modificada en 2004, 2005 y 2006	El artículo 2 establece los principios de legalidad, buena fe y deber de asegurar la calidad de los datos personales. El artículo 4 establece las circunstancias bajo las cuales pueden procesarse datos personales. Un se ellas es obtener el consentimiento del titular. Los artículos 17 a .. Establecen los deberes de los responsables del tratamiento de datos. Dentro de tales obligaciones estás: - registrase ante la Comisión (art. 17 y 18) - informar al titular sobre su idenidad como responsable de los datos, la información obtenida y su uso (art. 19 y 20) - permitir el acceso a la información por parte de su titular	Los artículos 26 a 28 consagran el derecho de acceso El artículo 28a consagra el derecho de exigir la rectificación, supresión o bloquear la utilización de la información incorrecta, inexacta o desactualizada. El artículo 34a consagra el derecho de objeción al procesamiento de la información por motivos legítimos o porque esta será usada para marketing directo	El artículo 2 establece las características de calidad que deben tener los datos personales: - debe ser proporcionales a los propósitos para los que fueron obtenidos - debe ser destruidos o ajustados en caso de ser imprecisos o desproporcionados - deben ser conservados durante un tiempo necesario para el desarrollo de su finalidad El artículo 23 establece la obligación de quienes manejen los datos personales de adoptar las medidas técnicas y organizacionales necesarias para asegurar el adecuado manejo de los datos.	El artículo 6 crea la Commission for Personal Data Protection, autoridad encargada de supervisar el cumplimiento de la norma. Los artículos 7 a 16 establecen la composición y funciones de la Comisión. Los artículos 38 y 39 establecen los procedimientos administrativo y judicial para reclamar la protección de los derechos del titular Los artículos 42 y siguientes establecen las sanciones susceptibles de imponerse ante incumplimientos de la Ley

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

Chipre Processing of Personal Data (Protection of the Individual) Law of 2001 modificada por la Ley 37(I)/2003	La sección 4 establece los principios de legalidad, finalidad, el deber de asegurar la calidad de los datos personales y la obligación de eliminar los datos procesados en contra de la ley. La sección 5 establece las condiciones para procesar legamente los datos, dentro de las cuales se encuentra como regla general el deber de obtener el consentimiento del titular. La sección 7 establece el deber del responsable del tratamiento de datos, de notificar a la autoridad competente antes de iniciar su procesamiento. La sección 10 establece el deber de confidencialidad en el tratamiento de datos La sección 11 exige al responsable del tratamiento, informar al titular sobre la obtención y utilización de los datos personales	La sección 11 consagra el derecho de información del titular La sección 12 consagra el derecho de acceso a la información sobre los datos personales, así como el derecho de exigir la rectificación, supresión o bloqueen la utilización de la información incorrecta, inexacta o desactualizada, o que fue obtenida de manera ilegal. La sección 13 consagra el derecho de objeción al procesamiento de la información por motivos legítimos.	En cuanto a la calidad de los datos personales la sección 4 exige que estos sea: - relevantes y apropiados y no excesivos para la finalidad buscada. - exactos y actualizados - conservados durante un tiempo necesario para el desarrollo de su finalidad. La sección 10 establece el deber de adoptar las medidas técnicas y organizacionales necesarias para asegurar el adecuado manejo de los datos. Igualmente exige que los datos sean procesados de manera confidencial.	La sección 16 consagra el derecho del titular de solicitar medidas cautelares a una autoridad judicial, para proteger sus derechos. La sección 17 consagra el derecho del titular a ser compensado por daños sufridos. Las secciones 18 a 24 crean y regulan las funciones del Commissioner for Personal Data Protection. Autoridad encargada de supervisar el cumplimiento de la norma. Las secciones 25 y 26 contemplan sanciones administrativas y penales ante el incumplimiento de la norma
Croacia Act on personal data protection	El artículo 6 obliga a quien procese datos personales a hacerlo acorde a los principios de legalidad, finalidad	El artículo 19 establece el derecho de acceso a las información El artículo 20	En cuanto a la calidad de los datos, el artículo 6 exige que estos sean: - relevantes y suficientes (no	Los artículos 24 a 26 consagran la posibilidad para el titular de los datos, de solicitar la protección de sus

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

(Official Gazette, No. 103/03) Dinamarca Act 429 of 2000 Ha sido modificado en numerosas ocasiones, siendo la última el Act 1245 of 2012.	y verificando la calidad de los datos obtenidos. El artículo 7 establece como regla general el deber de obtener el consentimiento del titular de los datos para su procesamiento. El artículo 9 exige al responsable del tratamiento, informar al titular sobre la obtención y utilización de los datos personales La sección 5 obliga a quien procese datos personales a hacerlo acorde a los principios de buenas prácticas, finalidad y calidad de los datos. La sección 6 establece como regla general el deber de obtener el consentimiento del titular de los datos para su procesamiento Las secciones 28 y 29 exigen al responsable del tratamiento, informar al titular sobre la obtención y utilización de los datos personales Las secciones 43 y 48 establecen el deber del responsable del tratamiento de datos, de notificar a	consagra el derecho de exigir la completar, modificar o eliminar los datos incompletos, inexactos o desactualizados. El artículo 21 establece el derecho de objetar el procesamiento de datos personales con fines de mercadeo directo. La sección 31 consagra el derecho al acceso a la información sobre los datos personales La sección 35 consagra el derecho de objetar el procesamiento de los datos personales La sección 37 consagra el derecho de exigir la rectificación, eliminar o bloquear los datos incorrectos o desactualizados	excesivos) para la finalidad buscada. - exactos, completos y actualizados - conservados durante un tiempo necesario para el desarrollo de su finalidad. Los artículos 10 y 33 consagran los deberes de adoptar las medidas técnicas y organizacionales necesarias para asegurar el adecuado manejo de los datos. En cuanto a la calidad de los datos la sección 5 exige que estos sean: - adecuados, relevantes y no excesivos en relación con la finalidad para la que son recolectados - actualizados y exactos - conservados durante un tiempo necesario para el desarrollo de su finalidad. Las secciones 41 y 42 establecen la obligación de quienes manejen los datos personales de adoptar las medidas técnicas y organizacionales necesarias para asegurar el adecuado manejo de los datos.	derechos ante la Personal Data Protection Agency (procedimiento administrativo) Los artículos 27 a 35 crean y regulan las funciones de la Personal Data Protection Agency. Finalmente, los artículos 36 y siguientes establecen sanciones penales ante el incumplimiento de la norma. Las secciones 55 a 66 crean y regulan las funciones de la autoridad encargada de vigilar el cumplimiento de la norma: The Data Protection Agency. Adicionalmente, las secciones 67 y 68 establecen que la Dnish Court Administration supervisará el tratamiento de datos de las Cortes. Las secciones 69 y siguientes establecen las sanciones susceptibles de imponerse ante el incumplimiento de la norma.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

	la autoridad competente antes de iniciar su procesamiento			
Eslovaquia Act 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts.	Las secciones 6 a 9 establecen las obligaciones del responsable del tratamiento de la información La sección 11 establece como regla general la obligación de obtener el consentimiento del titular para procesar la información La sección 15 establece la obligación del responsable del tratamiento de datos, de informar al titular de los mismos, previo a su utilización. La sección 22 establece la obligación de mantener la confidencialidad de la información. Secciones 33 a 42 regulan la obligación de los responsables del tratamiento de datos de registrar sus actividades ante la autoridad competente	La sección 5 establece que el tratamiento de datos personales puede realizarse siempre y cuando se protejan derechos fundamentales como el derecho a la dignidad y a la privacidad La sección 28 consagra los siguientes derechos: - de acceso a la información -de exigir la rectificación o eliminación de datos inexactos, incompletos o desactualizados - objeción al procesamiento de datos para marketing directo o por motivos legítimos	La sección 16 exige que los datos sean veraces, exactos y que estén actualizados La sección 19 establece que el responsable del tratamiento de datos responderá por la seguridad en el manejo de los datos.	Las secciones 23 a 27 y 45 a 51crean y regulan la autoridad para la supervisión del cumplimiento de la norma: Office for Personal Data Protection. Las secciones 62 a 67 consagran los procedimientos para proteger los derechos de los titulares de los datos. Las secciones 68 y siguientes establecen las sanciones (multa y sanciones disciplinarias) ante violaciones de los derechos de los titular de los datos personales.
Eslovenia Personal Data Protection Act (ZVOP-1) 2004	Los artículos 2 a 4 establecen los principios de legalidad, justicia, proporcionalidad y no discriminación en el procesamiento	El artículo 30 establece el derecho de acceso a la información sobre datos personales	El artículo 18 exige que los datos sean exactos y estén actualizados El artículo 21 estipula que los datos	El artículo 34 establece la protección judicial de los derechos de los titulares de lo datos.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

	de datos personales El artículo 16 establece el principio de finalidad El artículo 19 establece la obligación del responsable del tratamiento de datos, de informar al titular de los mismos, previo a su utilización. El artículo 27 establece el deber del responsable del tratamiento de datos, de notificar a la autoridad competente antes de iniciar su procesamiento El artículo 30 establece la obligación del responsable del tratamiento de datos, de informar al titular de los mismos, previo a su utilización.	El artículo 33 establece el derecho de exigir la corrección, bloqueo, eliminación y objeción de los datos por parte del titular	personales solo pueden ser conservados durante un tiempo necesario para el desarrollo de su finalidad. Los artículos 24 y 25 establecen la obligación de quienes manejan los datos personales de adoptar las medidas técnicas y organizacionales necesarias para asegurar el adecuado manejo de los datos.	Los artículos 37 a 49 crean y regulan las funciones del National Supervisory Body for Personal Data Protection, entidad encargada de vigilar el cumplimiento de la norma. Los artículos 91 y siguientes establecen las sanciones susceptibles de imponerse ante el incumplimiento de la norma.
Estonia Personal Data Protection Act 2008	La sección 6 establece los principios generales para el tratamiento de datos personales: - legalidad - finalidad - proporcionalidad - uso restringido (se requiere el consentimiento del titular o la autorización de la autoridad competente (secciones 10 y 12))	Las secciones 19 y 20 regulan el derecho de acceso a la información por parte del titular La sección 21 consagra el derecho derecho de exigir la corrección, bloqueo, eliminación de datos inexactos y obtenidos de manera ilegal.	En cuanto al principio de alta calidad que debe tener los datos procesados, la sección 6 exige que estos sean actualizados, completos y necesarios para alcanzar la finalidad propuesta. La sección 6 exige la adopción de medidas necesarias para proteger los datos de	Las secciones 22 y 23 establecen el derecho del titular de los datos a acudir a la autoridad administrativa o judicial competente para reclamar la protección de sus derechos Las secciones 32 a 41 crean y regulan la funciones del Data Protection Inspectorate.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

	- alta calidad de los datos - principio de seguridad - principio de participación del titular de los datos (quien procese los datos debe informar de este hecho al titular (sección 15)) Las secciones 27 a 29 establecen el deber del responsable del tratamiento de datos sensibles, de notificar a la autoridad competente antes de iniciar su procesamiento		usos indebidos o ilegales (secciones 24, 25 y 26)	Autoridad encargada de vigilar el cumplimiento de la norma. Las secciones 42 a 44 establecen las responsabilidades y sanciones susceptibles de imponerse ante el incumplimiento de la norma.
Finlandia Act 523/1999 Personal Data Act	La sección 5 establece el deber de quien procese datos personales, de actuar con cuidado y legalmente La sección 6 establece el principio de finalidad y exclusividad en el uso de los datos personales La sección 8 establece como regla general la obligación de obtener el consentimiento del titular para procesar la información La sección 24 establece la obligación del responsable del	La sección 26 establece el derecho de acceso a la información sobre los datos personales La sección 29 establece el derecho de exigir la rectificación o eliminación de datos incorrectos La sección 30 establece el derecho de prohibir el procesamiento de datos con fines de publicidad, ventas, mercadeo, etc.	La sección 9 establece los principios relacionados con la calidad de los datos: necesidad y adecuación Las secciones 32 a 35 establecen las reglas sobre la seguridad de los datos	Los artículos 38 a 46 crean la autoridad supervisora: Office of the Data Protection Ombudsman; y regulan sus funciones. Las secciones 47 y 48 establecen las sanciones ante el incumplimiento de las normas sobre protección de datos personales.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

	tratamiento de datos, de informar al titular de los mismos, previo a su utilización Las secciones 36 y 37 establecen el deber del responsable del tratamiento de datos, de notificar a la autoridad competente antes de iniciar su procesamiento			
Francia Ley 78-17 del 6 de enero de 1978. Ha sido modificada en multiples ocasiones, siendo la ultima la Ley 2013-907 del 11 de octubre de 2013	El artículo 6 establece los principios generales de legalidad, finalidad. El artículo 7 establece por regla general la obligación de obtener el consentimiento del titular para poder utilizar sus datos personales. Según los artículos 22 y siguientes, los responsables del tratamiento de datos personales están obligados a declarar ante la Comisión para obtener su autorización, previo al procesamiento de la información. El artículo 32 establece la obligación de los responsables del tratamiento de los datos personales, de informar previamente a los	El artículo 38 establece el derecho del titular de oponerse, por motivos legítimos, a la utilización de sus datos personales. El artículo 39 consagra el derecho de acceso a los datos personales. El artículo 40 consagra los derechos de exigir la rectificación, modificación, actualización, bloqueo o supresión de la información inexacta, incompleta o equívoca.	El artículo 6, además de los principios generales de legalidad y finalidad, establece las condiciones bajo las cuales de asegura la calidad de los datos personales. Establece que los datos personales deben ser adecuados, pertinentes y no excesivos en relación con las finalidades para las que fueron obtenidos. Afirma que deben ser exactos, completos y actualizados. Por último, deben ser conservados durante un tiempo necesario para el desarrollo de su finalidad. El artículo 34 obliga a los responsables del tratamiento de datos personales a tomar las medidas para verificar la seguridad de la información.	Los artículos 11 a 21 crean la Commission nationale de l'informatique et des libertés y establecen sus funciones. Los artículos 45 a 49 establecen las sanciones que puede imponer la Commission nationale de l'informatique et des libertés. Los artículos 50 a 52 regulan las sanciones penales susceptibles de imponerse.

	titulares sobre el uso de sus datos.			
Grecia Ley 2472/1997 (Protection of Individuals with regard to the Processing of Personal Data)	El artículo 4 establece los principios de legalidad, finalidad y calidad de la información. Además afirma el deber del responsable de los datos de cumplir con dichos principios. El artículo 5 establece por regla general la obligación de obtener el consentimiento del titular para poder utilizar sus datos personales. Según el artículo 6, los responsables del tratamiento de datos personales deben notificar a la Autoridad la intención de procesar determinados datos El artículo 10 establece el deber de mantener la confidencialidad de los datos. El artículo 11 establece el deber del responsable del tratamiento de informar al titular de los datos la naturaleza de los mismos y las condiciones de recopilación.	El artículo 12 consagra el derecho de acceso del titular El artículo 13 consagra el derecho de objeción al procesamiento de los datos El artículo 14 consagra el derecho de solicitar medidas cautelares de protección de los derechos del titular	En cuanto a la calidad de la información el artículo 4 exige que esta sea: - adecuada, relevante y no excesiva en relación su finalidad - exacta y actualizada - conservada durante un tiempo necesario para el desarrollo de su finalidad. El artículo 10 establece el deber del responsable de los datos de implementar las medidas necesarias para asegurar el uso adecuado de los datos.	Los artículos 15 a 20 crean y regulan las funciones de la autoridad supervisora de la normatividad.- The Personal Data Protection Authority Los artículos 21 y siguientes establecen las sanciones administrativa y penales ante el incumplimiento de la normatividad
Hungría	La sección 4 establece que todo	La sección 14 consagra los	Sobre la calidad de los datos la sección 4	La sección 22 establece un

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information	tratamiento de datos personales debe seguir los principios de finalidad, legalidad y proteger la calidad de los datos. La sección 5 establece como regla general el deber de obtener el consentimiento de los titulares de los datos, previo su uso. Las secciones 15 y 20 consagran la obligación de los responsables del tratamiento de datos de informar a los titulares sobre la naturaleza de los datos y las condiciones de obtención. La sección 17 obliga quienes procesen datos personales a velar por la protección de los derechos de los titulares de los mismos.	siguientes derechos del titular de los datos personales: - derecho de acceso - derecho de exigir la rectificación, eliminación o bloqueo de datos La sección 21 consagra el derecho de objetar el procesamiento de los datos bajo determinadas circunstancias	consagra que estos deben ser exactos, completos y actualizados La sección 7 exige a quienes procesen datos personales, tomar todas las medidas necesarias para proteger los datos de usos indebidos.	mecanismo judicial para exigir la protección de los derecho del titular de los datos. Las secciones 38 a 51 crean y regulan las funciones de la autoridad encargada de velar por el cumplimiento de la norma: National Authority for Data Protection and Freedom of Information. Las secciones 52 y siguientes establecen los procedimientos para velar por el cumplimiento de la norma.
Irlanda Data Protection Act 1988, modificada por el Data Protection Amendment Act 2003	La sección 1 establece que todo tratamiento de datos personales debe seguir los principios de justicia, finalidad y proteger la calidad de los datos. La sección 2A establece como regla general el deber de obtener el consentimiento de los titulares de los datos, previo su uso.	La sección 4 establece el derecho de acceso a la información. La sección 6 establece el derecho a exigir la rectificación o eliminación de datos incorrectos. Asimismo, de objetar el procesamiento de los datos en caso de que este pueda	Sobre la calidad de los datos la sección 1 consagra que estos deben ser exactos, completos y actualizados. También deben ser adecuados, relevantes y no excesivos en relación con su finalidad. por último, deben ser conservados durante un tiempo necesario para el desarrollo de su finalidad.	La sección 9 crea la autoridad competente para supervisar el cumplimiento de la Ley: The Data Protection Commissioner. Las secciones 10 a 15 establecen las funciones del comisionado Las secciones 26 a 31 establecen los

		causar daños al titular.	La sección 2C obliga a los responsables del tratamiento de datos a tomar las medidas técnicas y organizacionales necesarias para velar por la seguridad de los datos.	procedimientos para resolver eventuales conflictos y las sanciones en caso de incumplimiento de la norma.
Italia Data Protection Code - Legislative Decree no. 196/2003	Las secciones 10 y 13 obligan a los responsables del tratamiento de datos, informar a los titulares las características y condiciones de obtención de los datos. La sección 11 establece los principios de legalidad y finalidad. La sección 23 establece como regla general la obtención del consentimiento del titular para el tratamiento de datos personales por entes privados.	La sección 1 consagra el derecho de todas las personas a la protección de los datos personales. La sección 2 reconoce los derecho fundamentales en relación con la confidencialidad, identidad personal y protección de los datos personales. El título II consagra los derechos de los titulares como son: - El derecho de acceso a la información (sección 7-2 a)) - El derecho de exigir la rectificación, actualización (sección 7-3 a)) - El derecho a exigir la supresión, anonimato o bloqueo de la información procesada ilegalemente (sección 7 b)) - El derecho de objeción (sección 7-4)	La sección 11 establece los requisitos para manejar los datos y asegurar su calidad. Además de los principios de legalidad y finalidad se exige la exactitud de los datos, que estos sean relevantes, completos y no excesivos en relación con su finalidad. Por último, deben ser conservados durante un tiempo necesario para el desarrollo de su finalidad. Las secciones 31 a 36 establecen las medidas que deben tomarse para velar por la seguridad de los datos.	Las secciones 8 y 9 establecen mecanismos para que los titulares exijan la protección de sus derechos. La sección 15 afirma la responsabilidad de quienes procesan datos personales, por los daños que puedan causar. Las secciones 141 a 152 establecen mecanismos administrativos, no judiciales y judiciales para la solución de controversias que puedan presentarse. Las secciones 153 y siguientes crean y regulan las funciones de la autoridad encargada de la vigilancia del cumplimiento de la norma: The Garante per la Protezione dei Dati Personali Finalmente las secciones 161 a 172 establecen las sanciones administrativas y penales por incumplimiento del

				Código.
Letonia Personal Data Protection Law 2000	El artículo 7 establece las condiciones para el tratamiento legal de datos Los artículos 8 y 9 establecen la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos. El artículo 10 establece la obligación de quienes procesen datos personales de hacerlo de acuerdo a los principios de legalidad y finalidad. Así como asegurar la calidad de los datos.	El artículo 6 consagra el derecho de toda persona a la protección de sus datos personales El artículo 15 consagra el derecho de acceso a la información de los datos por parte del titular El artículo 16 consagra el derecho a exigir la rectificación o supresión de información incompleta, incorrecta o que ha sido procesada de forma ilegal. El artículo 19 consagra el derecho a objetar el procesamiento de la información cuando los datos serán utilizados para fines comerciales	En cuanto a la calidad de los datos el artículo 10 exige que estos sean: - exactos y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. El artículo 14 exige establecer las medidas necesaria para asegurar el uso adecuado de los datos	El artículo 32 establece el derecho del titular de los datos de obtener compensación en caso de sufrir un daño. Los artículos 29 a 32 crean y regulan las funciones del Data State Inspectorate. Autoridad encargada de vigilar el cumplimiento de la Ley.
Lituania Law No. I-1374 of 1996 on Legal Protection of Personal Data (nueva versión Law No. X-1444 2008	El artículo 3 establece la obligación de quienes procesen datos personales de hacerlo de acuerdo a los principios de legalidad y finalidad. Así como asegurar la calidad de los datos. El artículo 5 establece las condiciones para el tratamiento legal de	El artículo 23 consagra el derecho de acceso a la información de los datos por parte del titular (art. 25). Asimismo consagra el derecho a exigir la rectificación o supresión de la información (art. 26). así como el derecho a objetar el procesamiento de la misma	En cuanto a la calidad de los datos el artículo 3 exige que estos sean: - idénticos, adecuados y no excesivos en relación con la finalidad - exactos y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. El artículo 30 exige	El artículo 23 establece el derecho del titular de los datos a quejarse ante la autoridad competente por la vulneración de sus derechos. Los artículos 36 a 41 crean y regulan las funciones del State Data Protection Inspectorate. Autoridad encargada

	datos Los artículos 23 y 24 establecen la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos. El artículo 31 establece el deber del responsable del tratamiento de datos personales de notificar a la autoridad competente, antes de adelantar dicho tratamiento	(art.27).	establecer las medidas necesaria para asegurar el uso adecuado de los datos	de vigilar el cumplimiento de la Ley. Los artículos 53 y 54 establecen sanciones ante el incumplimiento de la norma.
Luxemburgo Loi du 2 août 2002 relative à la protection des personnes à l'egard du traitement des données à caractère personnel (modifiée par: loi du 31 juillet 2006, la loi du 22 decembre 2006, la loi du 27 juillet 2007.)	El artículo 4 establece la obligación de quienes procesen datos personales de hacerlo de acuerdo a los principios de legalidad y finalidad. Así como asegurar la calidad de los datos. El artículo 5 establece las condiciones para el tratamiento legal de datos El artículo 26 establece la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de	El artículo 28 consagra el derecho de acceso a la información de los datos por parte del titular Los artículos 28 y 42 consagran el derecho a exigir la rectificación o supresión de la información incompleta, inexacta u obtenida de forma ilegal. El artículo 30 consagra el derecho a objetar el procesamiento de la información cuando existan motivos legítimos	En cuanto a la calidad de los datos el artículo 4 exige que estos sean: - adecuados, pertinentes y no excesivos en relación con la finalidad - exactos y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. Los artículos 22 a 25 exigen establecer las medidas necesaria para asegurar el uso adecuado de los datos	Los artículos 32 y 34 a 37 crean y regulan las funciones de la Commission nationale pour la protection des données. Autoridad encargada de vigilar el cumplimiento de la Ley. Los artículos 33, 38 y 39 establecen los mecanismos de solución de controversias

	los datos obtenidos. El artículo 12 establece el deber del responsable del tratamiento de datos personales de notificar a la autoridad competente, antes de adelantar dicho tratamiento			
Malta	La sección 7 establece la obligación de quienes procesen datos personales de hacerlo de acuerdo a los principios de legalidad, buenas prácticas y finalidad. Así como asegurar la calidad de los datos. Las secciones 19 y 20 establecen la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos. La sección 29 establece el deber del responsable del tratamiento de datos personales de notificar a la autoridad competente, antes de adelantar dicho tratamiento	La sección 21 consagra el derecho de acceso a la información de los datos por parte del titular La sección 22 consagra el derecho a exigir la rectificación, bloqueo o supresión de la información La sección 11 consagra el derecho a objetar el procesamiento de los datos .	En cuanto a la calidad de los datos la sección 7 exige que estos sean: - adecuados, relevantes y no excesivos en relación con la finalidad - correcto, necesario y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. La sección 26 exige establecer las medidas necesaria para asegurar el uso adecuado de los datos	Los artículos 36 a 41 crean y regulan las funciones del Information and Data Protection Commissioner. Autoridad encargada de vigilar el cumplimiento de la Ley. Los artículos 41a 41b, 46 y 47 establecen sanciones ante el incumplimiento de la norma.
Paises Bajos Personal Data	El artículo 6 establece el principio de legalidad para el	El artículo 33 consagra el derecho del titular a que se le informe	Los artículos 9, 10 y 11 consagran las reglas que garantizan la calidad de los	Los artículos 45 a 50 establecen mecanismos administrativos y

Protection Act (Act of 6 July 2000, Bulletin Of Acts, Orders And Decrees 302, Containing Rules Regarding The Protection Of Personal Data)	procesamiento de datos personales. El artículo 7 consagra la obligación de utilizar los datos para fines específicos y legítimos (finalidad) El artículo 8 establece las condiciones en que está permitido el tratamiento de datos personales. Dentro de estas se exige la obtención del consentimiento inequívoco del titular. El artículo 12 establece la obligación de confidencialidad de quien maneja datos personales. Los artículos 27 y 28 establecen el deber del responsable del tratamiento de datos personales de notificar a la Comisión de Protección de Datos, antes de adelantar dicho tratamiento	previamente sobre el uso que se dará a los datos recolectados. Según el artículo 34, el titular también deberá ser informado sobre las circunstancias en que fue recolectada la información. Los artículos 35 y 36 establecen los derechos de acceder, corregir, modificar, completar, rectificar o suprimir los datos personales por parte de su titular. El artículo 40 establece el derecho de objeción de los datos por parte del titular	datos. Los artículos 13 y 14 exigen implementar las medidas técnicas y organizacionales para proteger los datos personales de pérdida o uso ilegal.	judiciales a los que los titulares de los datos personales pueden acudir para proteger sus derechos o ser indemnizados por daños sufridos. Los artículos 51 a 61 establecen las funciones y composición de la autoridad encargada de supervisar el cumplimiento de la ley. Esta autoridad es la Data Protection Commission.
Polonia Act on the Protection of Personal Data, 1997. Modificado en numerosas ocasiones	El artículo 23 establece las condiciones bajo las cuales se pueden procesar datos personales y obliga a los responsables del tratamiento a obtener el consentimiento de los titulares de los	El artículo 1 establece el derecho de toda persona a la protección de sus datos personales. El artículo 32 consagra los siguientes derechos del titular de la	El artículo 26 establece las condiciones para asegurar la calidad de los datos así: - los datos deben ser relevantes y adecuados en relación con finalidad de su recolección. - deben ser	Los artículos 8 a 22 crean y establecen las funciones de la autoridad supervisora denominada Inspector General for Personal Data Protection Los artículo 49 a 54

siendo la última la Ley 230 de 2011	mismos. Los artículos 24 y 25 establecen la obligación de quienes procesan datos personales de informar a los titulares sobre su naturaleza y condiciones de recopilación. El artículo 26 consagra los principios de legalidad, finalidad, y calidad de los datos. El artículo 35 obliga al responsable del tratamiento a velar por protección de los derecho del titular y por la calidad y seguridad de los datos.	información: - el derecho de acceso a la información - el derecho a exigir la modificación, actualización, rectificación y supresión de información incompleta, desactualizada o incorrecta - el derecho de exigir el bloqueo de la información en determinadas situaciones - el derecho de objetar el tratamiento de los datos para mercadeo o para ser transferidos a un tercero.	conservados durante un tiempo necesario para el desarrollo de su finalidad. El artículo 36 obliga a quienes procesen datos personales a adoptar las medidas necesarias para proteger el uso de los mismos.	establecen las sanciones susceptibles de imponerse ante el incumplimiento de la normas en la materia.
Portugal Act 67/98 on the Protection of Personal Data	El artículo 2 establece que el tratamiento de datos personales debe ser adelantado de manera transparente y respetando el derecho a la privacidad y otros derechos fundamentales. El artículo 6 establece la obligación de los responsables del manejo de datos de obtener el consentimiento del titular de manera clara y sin ambigüedad. El artículo 10 obliga a los responsables	El artículo 11 consagra el derecho acceso a la información. El artículo 12 establece el derecho de objetar el tratamiento de los datos su existen motivos legítimos e imperiosos.	El artículo 5 establece los principios para asegurar la calidad de los datos sean adecuados, relevantes y no excesivos en relación con su finalidad. También deben ser exactos y estar actualizados Por último, deben ser conservados durante un tiempo necesario para el desarrollo de su finalidad. El artículo 14 exige la implementación de medidas para proteger los datos personales de usos indebidos o	El artículo 21 y siguientes regulan lo concernante a la autoridad encargada de velar por el cumplimiento de la norma: La Comissão Nacional de Protecção de Dados Los artículos 35 a 49 establecen las sanciones administrativas y penales que pueden imponerse ante el incumplimiento de la norma.

	del tratamiento, a informar al titular sobre la obtención de sus datos El artículo 17 obliga a quienes procesan datos personales, conservar la confidencialidad de los mismos		legales. El artículo 15 contempla medidas especiales de seguridad para el manejo de datos sensibles.	
Reino Unido Data Protection Act 1998	El schedule 1 que desarrolla la sección 4, establece los principios de legalidad y finalidad. La sección 17 establece la obligación de los responsables del tratamiento de registrarse e informar a la autoridad competente sobre el procesamiento de datos.	En la parte II (secciones 7 a 15) se establecen los siguientes derechos de los titulares: - Derecho de acceso (sec. 7, 8 y 9) - Derecho de evitar el procesamiento de datos que puedan causar daño (sec. 10) - Derecho a evitar el procesamiento de datos con fines de mercadeo directo (sec. 11) - Derecho a obtener compensación por daños (sec. 13) - Derecho de rectificación, bloque, supresión y destrucción (sec. 14)	La sección 4 es desarrollada en el Schedule 1, el cual establece los principios generales de legalidad y finalidad. Exige también requisitos para asegurar la calidad de los datos como que estos sean adecuados, relevantes y no excesivos en relación con su finalidad. Los datos deben ser exactos, actualizados y deben ser conservados durante un tiempo necesario para el desarrollo de su objeto. También exige la adopción de medidas apropiadas contra el uso ilegal o no autorizado de los datos.	La sección 6 crea la autoridad competente en la materia, denominada Information Commissioner Las secciones 40 a 53 establecen los mecanismos mediante los cuales el Commissioner ejerce sus funciones de inspección y vigilancia. Las secciones 55 y 60 establecen las sanciones aplicables a quienes incumplen la norma.
República Checa Act No. 101/2000 Coll., Personal Data Protection Act	El artículo 5 establece las obligaciones del responsable del tratamiento datos, dentro de las cuales se encuentran: - asegurar la calidad de los datos - recolectar datos de acuerdo al principio de finalidad - obtener el	El artículo 12 consagra el derecho de acceso a la información de los datos por parte del titular El artículo 21 consagra el derecho a exigir la rectificación o supresión de información	En cuanto a la calidad de los datos el artículo 5 exige que estos sean: - exactos y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. Los artículos 13 a 15 exigen establecer las	Los artículos 28 a 43 crean y regulan las funciones del Office for personal data protection. Autoridad encargada de vigilar el cumplimiento de la Ley. Los artículos 44 y 46 establecen sanciones ante el

	consentimiento del titular de los datos velar porque se protejan los derechos del titular (art. 10) El artículo 11 establece la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos. El artículo 16 establece la obligación del responsable del tratamiento de datos de notificar a la autoridad competente, antes de adelantar dicho tratamiento	incompleta, incorrecta o que haya sido procesada de forma ilegal.	medidas necesarias para asegurar el uso adecuado de los datos	incumplimiento de la norma.
Rumania Law 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data	El artículo 4 establece los principios de legalidad, finalidad y deber de asegurar la calidad de los datos. El artículo 5 exige como regla general para quienes procesen datos, obtener el consentimiento del titular de los mismos. El artículo 12 establece el deber del responsable del tratamiento de informar a los titulares sobre su identidad como	El artículo 13 consagra el derecho de acceso a la información sobre los datos El artículo 14 consagra el derecho a exigir la rectificación, actualización, bloqueo y supresión de información incompleta, desactualizada o incorrecta. También consagra el derecho de solicitar convertir el anónima la información que no cumpla con la ley.	En cuanto a la calidad de los datos el artículo exige que estos sean: - adecuados, pertinentes y no excesivos en relación con la finalidad para la que fueron obtenidos - exactos y actualizados - conservados durante un tiempo necesario para el desarrollo de su objeto. El artículo 20 exige la implementación de medidas para proteger los datos personales de usos indebidos o ilegales.	El artículo18 consagra el derecho de acudir a los tribunales para reclamar la protección de los derechos del titular Los artículo 21 a 28 crean y regulan las funciones de The National Authority for the Supervision of Personal Data Processing Emidad encargada de vigilar el cumplimento de la norma. Los artículos 31 a 35 establecen las sanciones aplicables a quienes incumplen

	procesador de datos, sobre la naturaleza de los mismos y las condiciones en que se recopilaron. El artículo 19 consagra el deber de confidencialidad en el manejo de los datos El artículo 22 establece la obligación del responsable del tratamiento de datos de notificar a la autoridad competente, antes de adelantar dicho tratamiento.	El artículo 15 consagra el derecho a objetar el procesamiento de la información por motivos legítimos o cuando los datos serán utilizados para mercadeo directo		la norma.
Suecia Personal Data Act (1998:204)	La sección 9 establece la obligación de quienes procesen datos personales de hacerlo de acuerdo a los principios de legalidad, buena fe y finalidad. Así como asegurar la calidad de los datos. La sección 10 exige a quienes procesen datos, obtener el consentimiento del titular de los mismos. Las secciones 23 a 27 regulan el deber del responsable del tratamiento de informar a los titulares sobre los datos y las condiciones en que se recopilaron. La sección 36	Las secciones 26 y 28 establecen la responsabilidad de quienes procesan datos de permitir el acceso a la información por parte del titular, y de rectificar, bloquear o suprimir los datos procesados por fuera de las normas establecidas para ello.	La sección 9 establece las condiciones de calidad de los datos al exigir que estos: - sean adecuados y relevantes para el fin propuesto -no sean excesivos en relación con la finalidad - sean correctos y actualizados y en caso de no serlo, sean modificados o suprimidos. - no sean conservados por más tiempo del necesario, de acuerdo a la finalidad. La sección 31 exige la adopción de medidas técnicas y organizacionales para proteger los datos personales procesados.	Las secciones 43 a 47 crean una autoridad supervisora y establecen sus funciones. Las secciones 49 y siguientes establecen las sanciones posibles ante el incumplimiento de la normatividad en la materia.

	establece la obligación del responsable del tratamiento de datos de notificar a la autoridad competente, antes de adelantar dicho tratamiento			
No miembros de la Union Europea				
Albania Ley 9887/2008 on Protection of Personal Data	El artículo 5 establece la obligación de quienes procesen datos personales de hacerlo de acuerdo a los principios de legalidad y finalidad. Así como asegurar la calidad de los datos. El artículo 6 establece las condiciones para el tratamiento legal de datos, dentro de las cuales se encuentra como regla general, la obtención del consentimiento del titular. El artículo 18 establece la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos. Los artículos 19 y 20 establecen obligaciones del responsable y del encargado del tratamiento de datos.	El artículo 12 consagra el derecho de acceso a la información de los datos por parte del titular El artículo 13 consagra el derecho a exigir la rectificación, bloqueo o supresión de información incompleta, incorrecta o que haya sido procesada de forma ilegal. El artículo 15 consagra el derecho a objetar el procesamiento de la información por motivos legítimos o cuando los datos serán utilizados para mercadeo directo	En cuanto a la calidad de los datos el artículo 5 exige que estos sean: - adecuados y no excesivos en relación con la finalidad - exactos y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. El artículo 27 exige establecer las medidas necesaria para asegurar la confidencialidad, integridad y accesibilidad de los datos personales. El artículo 28 consagra el deber de tratamiento confidencial de los datos personales.	El artículo 16 establece el derecho del titular de los datos a quejarse ante la autoridad competente por la vulneración de sus derechos. El artículo 17 establece el derecho del titular a ser compensado en caso de sufrir un daño. Los artículos 29 a 38a crean y regulan las funciones del Commissioner for Personal Data Protection. Autoridad competente para vigilar el cumplimiento de la Ley. Los artículos 39 a 41 establecen sanciones administrativas ante el incumplimiento de la norma.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

	El artículo 21 establece la obligación de quienes procesan datos personales de notificar a la autoridad competente previo el procesamiento.			
Bosnia y Herzegovina Law on the Protection of Personal Data 2001	El artículo 4 establece la obligación de quienes procesan datos personales de hacerlo de acuerdo a los principios de legalidad y finalidad (art. 6) Así como asegurar la calidad de los datos. El artículo 5 establece las condiciones para el tratamiento legal de datos, dentro de las cuales se encuentra como regla general, la obtención del consentimiento del titular. El artículo 7 establece la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos.	El artículo 12 consagra el derecho de acceso a la información de los datos por parte del titular El artículo 13 consagra el derecho a exigir la rectificación o supresión de información incompleta, incorrecta o que ha sido procesada de forma ilegal	En cuanto a la calidad de los datos el artículo 4 exige que estos sean: - adecuados, relevantes y no excesivos en relación con la finalidad - exactos y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. Los artículos 10 y 11 exigen establecer las medidas necesaria para asegurar el uso adecuado de los datos	El artículo 18 establece el deber del responsable del tratamiento de datos de compensar a su titular en caso de sufrir un daño. Los artículos 19 a 23 crean y regulan las funciones de la Data Protection Commission. Autoridad encargada de vigilar el cumplimiento de la Ley. Los artículos 25 y 26 establecen sanciones administrativas ante el incumplimiento de la norma.
Macedonia Law on Personal Data Protection	El artículo 5 establece la obligación de quienes procesan datos personales de hacerlo de acuerdo a los principios de	El artículo 10 consagra el derecho de acceso a la información de los datos por parte del titular	En cuanto a la calidad de los datos el artículo 5 exige que estos sean: - agrupados, relevantes y no excesivos en relación	El artículo 18 establece el derecho del titular de los datos a quejarse ante la autoridad competente por la vulneración de sus

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

2005	legalidad y finalidad. Así como asegurar la calidad de los datos. El artículo 6 establece las condiciones para el tratamiento legal de datos, dentro de las cuales se encuentra como regla general, la obtención del consentimiento del titular. Los artículos 10 y 11 establecen la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos.	El artículo 14 consagra el derecho a exigir la rectificación o supresión de información incompleta, incorrecta o que ha sido procesada de forma ilegal. El artículo 17 consagra el derecho a objetar el procesamiento de la información cuando los datos serán utilizados para publicidad.	con la finalidad - exactos, completos y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. Los artículos 23 a 26 exigen establecer las medidas necesaria para asegurar el uso adecuado de los datos	derechos. El artículo 21 establece el deber del responsable del tratamiento de datos de compensar a su titular en caso de sufrir un daño. Los artículos 37 a 48 crean y regulan las funciones del Directorate for personal data protection. Autoridad encargada de vigilar el cumplimiento de la Ley. Los artículos 49 y 50 establecen sanciones ante el incumplimiento de la norma.
Montenegro Personal Data Protection Law 2009	El artículo 2 establece los principios de legalidad, finalidad, proporcionalidad. El artículo 10 establece las condiciones para el tratamiento legal de datos, dentro de las cuales se encuentra como regla general, la obtención del consentimiento del titular. Los artículos 20 y 21 establecen la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza.	Los artículos 10, 43 consagran el derecho de acceso a la información de los datos por parte del titular El artículo 44 consagran el derecho a exigir la rectificación, bloqueo o supresión de información incompleta, incorrecta o que ha sido procesada de forma ilegal.	El artículo 3 exige que los datos procesados sean: - exactos, completos y actualizados (art. 22) - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad (art. 18) Los artículos 24 a 25 exigen establecer las medidas necesaria para asegurar el uso adecuado de los datos	El artículo 47 establece el derecho del titular de los datos a quejarse ante la autoridad competente por la vulneración de sus derechos. El artículo 48 establece el derecho del titular a ser compensado en caso de sufrir un daño. Los artículos 49 a 73 crean y regulan las funciones del Commission for Personal Data Protection. Autoridad encargada de vigilar el cumplimiento de la Ley.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

	condiciones de recolección y uso de los datos obtenidos. Los artículos 27 y 28 establecen la obligación de quienes procesan datos personales de obtener autorización de la autoridad competente previo el procesamiento.			El artículo 74 establece sanciones ante el incumplimiento de la norma.
Noruega Personal Data Act Act of 14 April 2000 No. 31	La sección 19 establece la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos. Las secciones 31 a 35 establecen la obligación de quienes procesan datos personales de notificar a la autoridad competente previo el procesamiento. Asimismo, establecen la obligación de obtener un licencia para manejar datos personales sensibles.	La sección 18 establece el derecho de acceso del titular de los datos personales La sección 25 establece el derecho del titular afectado por una decisión basada en el procesamiento automático de datos, de solicitar la revisión por parte de una persona física. La sección 26 establece el derecho del titular de solicitar su exclusión de canales de mercadeo directo Las secciones 27 y 28 establecen los derechos de rectificación y supresión de datos	La sección 11 establece los requisitos para asegurar la calidad de los datos Las secciones 13 y 14 exigen establecer las medidas necesaria para asegurar la confidencialidad, integridad y accesibilidad de los datos personales.	La sección 42 crea la autoridad supervisora del manejo de datos personales: el Data Inspectorate Las decisiones de dicha entidad puede ser apeladas ante el Privacy Appeals Board Las secciones 47 a 49 establecen sanciones por el incumplimiento de la ley que van desde multas hasta la pena de prisión.
Islandia Acton the Protection of Privacy as regards the Processing of	El artículo 7 establece los principios de legalidad, finalidad y el deber de asegurar la calidad de los datos. El artículo 8	El artículo 18 consagra el derecho de acceso a la información de los datos por parte del titular El artículo 27 establece el	En cuanto a la calidad de los datos el artículo 7 exige que estos sean: - adecuados, relevantes y no excesivos en relación con la finalidad - confiables y	Los artículos 36 a 40 crean y regulan las funciones del Data Protection Authority. Autoridad encargada de vigilar el cumplimiento de la Ley.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

Personal Data, No. ??-2000	establece las condiciones para el tratamiento legal de datos, dentro de las cuales se encuentra como regla general, la obtención del consentimiento del titular. Los artículos 16, 20 y 21 establecen la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos. Los artículos 31 y 32 establecen la obligación de quienes procesan datos personales de notificar a la autoridad competente previo el procesamiento.	derecho del titular afectado por una decisión basada en el procesamiento automático de datos, de solicitar la revisión por parte de una persona física. El artículo 25 consagra el derecho a exigir la rectificación o supresión de información incompleta, incorrecta o que ha sido procesada de forma ilegal. El artículo 28 consagra el derecho a objetar el procesamiento de la información cuando existan motivos legítimos	actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. Los artículos 11 a 13 exigen establecer las medidas necesaria para asegurar el uso adecuado de los datos, y para procesarlos en forma confidencial.	Los artículos 41 a 43 establecen sanciones ante el incumplimiento de la norma.
Kosovo Law 03-L-172 of 2010 on Protection of Personal Data	El artículo 3 establece los principios de legalidad, finalidad y el deber de asegurar la calidad de los datos. El artículo 5 establece las condiciones para el tratamiento legal de datos. El artículo 10 establece la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza.	El artículo 22 consagra el derecho de acceso a la información de los datos por parte del titular El artículo 24 consagra el derecho a exigir la rectificación o supresión de información incompleta, incorrecta o que ha sido procesada de forma ilegal. El artículo 60 consagra el derecho a objetar el procesamiento	En cuanto a la calidad de los datos el artículo 3 exige que estos sean: - adecuados, relevantes y no excesivos en relación con la finalidad - exactos y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. Los artículos 14 a 16 exigen establecer las medidas necesaria para asegurar el uso adecuado de los datos.	El artículo 26 establece el derecho del titular de los datos a quejarse ante una autoridad judicial por la vulneración de sus derechos. Los artículos 29 a 50 crean y regulan las funciones del National Agency for Protection of Personal Data. Autoridad encargada de vigilar el cumplimiento de la Ley. Los artículos 79 a 91 establecen los

	condiciones de recolección y uso de los datos obtenidos. Los artículos 18 a 20 establecen la obligación de quienes procesan datos personales de notificar a la autoridad competente previo el procesamiento.	de la información cuando su destino sea el marketing directo		actos que constituyen violaciones de la norma y las respectivas sanciones
Serbia **Law on Personal Data Protection 2009**	El artículo 3 establece los principios de legalidad, finalidad y el deber de asegurar la calidad de los datos. El artículo 5 establece las condiciones para el tratamiento legal de datos. El artículo 15 establece la obligación del responsable del tratamiento de informar al titular de los datos sobre la naturaleza, condiciones de recolección y uso de los datos obtenidos. El artículo 49 establece la obligación de quienes procesan datos personales de notificar a la autoridad competente previo el procesamiento.	El artículo 20 consagra el derecho de acceso a la información de los datos por parte del titular El artículo 21 consagra el derecho del titular a obtener una copia de la información El artículo 22 consagra el derecho a exigir la rectificación modificación, actualización o supresión de información incompleta, incorrecta o que ha sido procesada de forma ilegal. Los artículos 27 y 28 establecen los procedimientos para ejercer los derechos	En cuanto a la calidad de los datos el artículo 3 exige que estos sean: - adecuados, relevantes y no excesivos en relación con la finalidad - exactos y actualizados - conservados por estrictamente el tiempo necesario, de acuerdo a la finalidad. Los artículos 46 y 47 exigen establecer las medidas necesaria para asegurar el uso adecuado de los datos.	El artículo 32 establece el derecho del titular de los datos a acudir ante la autoridad competente y solicitar la protección de sus derechos Los artículos 44 a 45 y 54 a 56. crean y regulan las funciones del Commissioner for Information of Public Importance and Personal Data Protection. Autoridad encargada de vigilar el cumplimiento de la Ley. El artículo 57 establece las sanciones ante el incumplimiento de la norma.
Suiza **Swiss Federal Act on Data**	El artículo 4 establece los principios de la legalidad, buena fe y finalidad.	En el artículo 5 se establece el derecho del titular a exigir la modificación de	Además de los principios generales del artículo 4 para el manejo de los datos, el artículo 5 exige que	El artículo 13 establece que el titular de los datos puede ejercer sus derechos ante un

Protection (DPA) 1992	Asimismo, el titular de los datos debe conocer de su recolección y, en ciertos casos, es necesario su consentimiento informado y voluntario. Según el artículo14 el responsable del tratamiento de datos sensibles está obligado a informar sobre su recolección. El artículo 18a obliga a los organismos federales a informar al titular sobre la recolección de datos personales.	los datos si estos son incorrectos. El artículo 8 establece el derecho de acceso por parte del titular. El artículo 20 establece el derecho de bloquear la divulgación de la información por parte de autoridades pública, si hay un interés legítimo para ello. Los artículos 15 y 25 establecen procedimiento para que los titulares de los datos puedan defender sus derechos de acceso, modificación o supresión de datos incorrectos.	los datos personales deben ser correctos y fiables. El artículo 7 exige tomar medidas técnicas y organizacionales para evitar el tratamiento no autorizado e inapropiado de los datos. El artículo 11 establece la posibilidad de crear una regulación para certificar la seguridad de los datos, e incluso se crear una etiqueta de seguridad para los datos.	ente privado, mediante un procedimiento judicial del Código de Procedimiento Civil de 2008 El artículo 25 se remite al procedimiento del Federal Act del 20 de diciembre de 1968, para adelantar acciones contra autoridades federales que manejen datos personales. El artículo 26 y siguientes establecen la composición y funciones del Federal Data Protection and Information Commissioner. Funcionario encargado de vigilar el cumplimiento de la Ley. Los artículos 333 a 35 establecen diferentes sanciones por el incumplimiento de la Ley.
Turquía	Actualmente no exsite una Ley que regule de manera general e integral el tratamiento de datos personales en Turquía. En consecuencia, la protección de datos personales se adelanta hay a partir de normas constitucionales (La sección 5 de la			

	Constitución de 1982 desarrolla el derecho a la privacidad) y de normas del Código Civil, Código Penal, normas laborales y regulaciones bancarias. Adicionalmente, en virtud del proceso de anexión de Turquía a la Unión Europea, existe un proyecto de ley de protección de datos personales desde 2005, pero este aun no ha sido aprobado por el parlamento.			

Con base en la información presentada en la tabla anterior, es posible concluir que los países que se enlistan a continuación son los que cuentan con un nivel adecuado de protección de datos personales. Lo anterior, con base en los criterios que fijó la Corte Constitucional de Colombia para determinar si un país cuenta con unos estándares mínimos de protección. Esto es que, tal como lo menciona la sentencia C-748 de 2012, cuentan con una legislación que contempla obligaciones y derechos de los responsables del tratamiento y de los titulares de los datos personales; define los principios de calidad y seguridad de los datos; establece una autoridad de control en materia de protección de datos con sus funciones y atribuciones.

Únicamente a estos países resulta procedente una transferencia internacional de datos, por contar todos ellos con una legislación que protege el derecho de habeas data de manera equivalente o superior al que lo hace la legislación Colombiana:

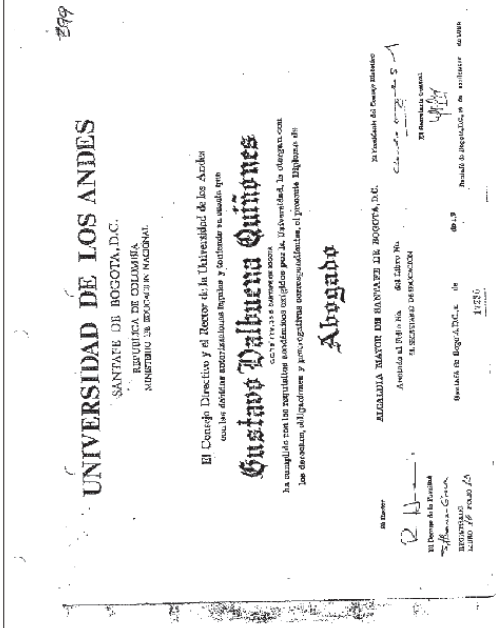
1. España
2. Alemania
3. Austria
4. Bélgica
5. Francia

6. Italia
7. Polonia
8. Portugal
9. Reino Unido
10. Suecia
11. Noruega
12. Suiza
13. México
14. Uruguay
15. Argentina
16. Nicaragua
17. Perú
18. Costa Rica
19. Estados Unidos
20. Canadá
21. Japón
22. Corea
23. Malasia
24. Nueva Zelanda
25. Rusia
26. Albania
27. República Checa
28. Rumania
29. Islandia
30. Montenegro
31. Bosnia
32. Macedonia
33. Servia
34. Cosovo
35. Singapur

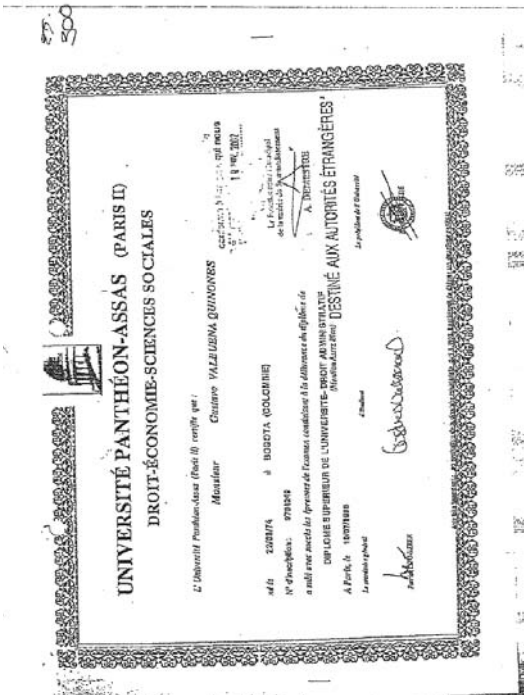
7. BIBLIOGRAFÍA

- The OECD Privacy Framework 2013
- Baker& Mckenzies Global Privacy Handbook 2013 edition
- Cerda Silva Alberto, Universidad de Chile: El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea" Revista de Derecho de la Pontificia Universidad Católica de Chile Agosto de 2011
- Álvarez Rigaudias Cecilia Artículo "Las transferencias internacionales de datos personales y el nivel equiparable o adecuado de protección" Madrid- 2010.
- Remolina Angarita Nelson, Tratamiento de datos personales aproximación internacional y comentarios a la Ley 1581 de 2012 primera edición- Legis. Bogotá, D.C.
- Dictamen 4/2002 del Grupo de Protección de Datos sobre el nivel de protección de datos personales en Argentina. Bruselas, 3 de octubre de 2002.
- Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46 del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act
- Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza
- Documento adoptado por el Grupo de Trabajo el 26 de junio de 1997 Primeras Orientaciones sobre la Transferencia de Datos personales a Terceros Países y las Posibles formas de evaluar la adecuación.
- Documento de Trabajo Transferencias de Datos Personales a Terceros Países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE aprobado por el Grupo de Trabajo el 24 de julio de 1998.
- Propuesta de Reglamento General de Protección de datos. Bruselas, 2012.
- Superintendencia de Industria y Comercio. Concepto 13-163296 de 28 de agosto de 2013
- http://www.agpd.es/portalwebAGPD/internacional/adecuacion/canada/index-ides-idphp.php

- PAVÓN, Juan Antonio. "La Protección de Datos Personales en el Consejo de Europa: El Protocolo Adicional al Convenio 108 Relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos Personales", Universidad de Extremadura, 2002. Encontrado en: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F831270.pdf&ei=6BuVUszmJ9KskAeLmYDAAw&usg=AFQjCNFf9v6R1JG8RYaQ-2v5mERpl_R70A&sig2=3sn0UT9XcQT1_rsRgngvBg&bvm=bv.57155469,d.eW0
- http://inicio.ifai.org.mx/Estudios/prot_datos.pdf
- http://www.redipd.org/la_red/Historia/index-ides-idphp.php


UNIVERSIDAD DE LOS ANDES
SANTAFE DE BOGOTA, D.C.
REPUBLICA DE COLOMBIA
MINISTERIO DE RELACIONES EXTERIORES

El Consejo Directivo y el Rector de la Universidad de los Andes
Gustavo Valbuena Quiñones
Abogado


UNIVERSITÉ PANTHÉON-ASSAS (PARIS II)
DROIT-ÉCONOMIE-SCIENCES SOCIALES
DIPLÔME SUPÉRIEUR DE L'UNIVERSITÉ DROIT ARMS STRATIF DESTINÉ AUX AUTORITÉS ÉTRANGÈRES

REPÚBLICA DE COLOMBIA

MINISTERIO DE EDUCACIÓN NACIONAL

RESOLUCIÓN NÚMERO 8323

28 DIC. 2006

Por medio de la cual se resuelve una solicitud de convalidación

LA DIRECTORA DE CALIDAD PARA LA EDUCACIÓN SUPERIOR (E)
en ejercicio de sus atribuciones legales y en especial las que le confiere el Decreto 2230 de 2003 y las Resoluciones No.2763 del 13 noviembre de 2003 y No.7300 del 8 de diciembre de 2005.

CONSIDERANDO:

Que GUSTAVO VALBUENA QUIÑONES, ciudadano colombiano, identificado con cédula de ciudadanía No.79.779.355, presentó para su convalidación el DIPLOME SUPERIEUR DE L'UNIVERSITE-DROIT ADMINISTRATIF, otorgado el 10 de julio de 1998 por la UNIVERSITÉ PANTHÉON -ASSAS (PARIS II), Francia, mediante solicitud radicada en el Ministerio de Educación Nacional con el No.2006ER67126-25819/06.

Que de conformidad con lo dispuesto en el Decreto 2230 de 2003, corresponde al Ministerio de Educación Nacional convalidar los títulos de educación superior otorgados por instituciones de educación superior extranjeras de acuerdo con las normas vigentes.

Que en virtud del artículo 3° de la Resolución 5547 del 1 de diciembre de 2005, uno de los criterios aplicables para efectos de la convalidación de títulos otorgados por instituciones de educación superior extranjeras, es el de Programa o Institución Acreditados, o su equivalente en el país de procedencia, el cual establece que *"Si la institución que otorgó el título que se somete a convalidación o si el programa académico cursado por el solicitante se encuentran acreditados, o cuentan con un reconocimiento equivalente por parte de una entidad certificadora o evaluadora de alta calidad, reconocida en el país de origen o a nivel internacional, se procederá a convalidar el título."*

Que consultado el "Academic Ranking of World Universities – 2006", sistema de evaluación de alta calidad, desarrollado por The Institute of Higher Education, Shanghai Jiao Tong University, que clasifica las mejores instituciones de educación superior del mundo, teniendo en cuenta criterios tales como el alto nivel de desempeño académico, el alto nivel de investigación, los reconocimientos internacionales y el número de publicaciones, se pudo establecer que la UNIVERSITÉ PANTHÉON -ASSAS (PARIS II), se encuentra clasificada entre las 500 mejores.

Que consultado el Comité National d'evaluation (CNE), entidad evaluadora y acreditadora de la educación superior en FRANCIA, se pudo establecer que la UNIVERSITE PANTHEON ASSAS (PARIS II), se encuentra acreditada.

Que con fundamento en las anteriores consideraciones y después de haber estudiado la documentación presentada, se concluye que es procedente la convalidación solicitada.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO.- Convalidar y reconocer para todos los efectos académicos y legales en Colombia, el título de DIPLOME SUPERIEUR DE L'UNIVERSITE-DROIT ADMINISTRATIF, otorgado el 10 de julio de 1998 por la UNIVERSITE PANTHÉON -ASSAS (PARIS II), Francia, a GUSTAVO VALBUENA QUIÑONES, ciudadano colombiano, identificado con cédula de ciudadanía No.79.779.355, como equivalente al título de ESPECIALISTA EN DERECHO ADMINISTRATIVO, que otorgan las instituciones de educación superior colombianas de acuerdo con la Ley 30 de 1992.

PARÁGRAFO.- La convalidación que se hace por el presente acto administrativo no exime al profesional beneficiario del cumplimiento de los requisitos exigidos por las normas que regulan el ejercicio de la respectiva profesión.

ARTÍCULO SEGUNDO.- La presente Resolución rige a partir de la fecha de su expedición y contra la misma procede el recurso de reposición, que debe ser presentado dentro de los cinco (5) días hábiles siguientes a su notificación de conformidad con el Código Contencioso Administrativo.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D. C., a los 28 DIC. 2006

LA DIRECTORA DE CALIDAD PARA LA EDUCACIÓN SUPERIOR (E),

ADRIANA MOLINA MANTILLA

RÉPUBLIQUE FRANÇAISE

DIPLÔME D'ÉTUDES APPROFONDIES

UNIVERSITÉ PARIS 1

M. GUSTAVO VALBUENA

REPÚBLICA DE COLOMBIA

MINISTERIO DE EDUCACIÓN NACIONAL

RESOLUCIÓN NÚMERO 8326

28 DIC. 2006

Por medio de la cual se resuelve una solicitud de convalidación

LA DIRECTORA DE CALIDAD PARA LA EDUCACIÓN SUPERIOR (E)
en ejercicio de sus atribuciones legales y en especial las que le confiere el Decreto 2230 de 2003 y las Resoluciones No.2763 del 13 noviembre de 2003 y No.7800 del 8 de diciembre de 2006.

CONSIDERANDO:

Que GUSTAVO VALBUENA QUIÑONES, ciudadano colombiano, identificado con cédula de ciudadanía No.79.779.355, presentó para su convalidación el DIPLOME D' ÉTUDES APPROFONDIES EN DROIT PUBLIC INTERNE, otorgado el 8 de diciembre de 1999 por la UNIVERSITÉ PARIS 1, Francia, mediante solicitud radicada en el Ministerio de Educación Nacional con el No.2006ER67125-25818/06.

Que de conformidad con lo dispuesto en el Decreto 2230 de 2003, corresponde al Ministerio de Educación Nacional convalidar los títulos de educación superior otorgados por instituciones de educación superior extranjeras de acuerdo con las normas vigentes.

Que en virtud del artículo 3° de la Resolución 5547 del 1 de diciembre de 2005, uno de los criterios aplicables para efectos de la convalidación de títulos otorgados por instituciones de educación superior extranjeras, es el de Programa o Institución Acreditados, o su equivalente en el país de procedencia, el cual establece que *"Si la institución que otorgó el título que se somete a convalidación o si el programa académico cursado por el solicitante se encuentran acreditados, o cuentan con un reconocimiento equivalente por parte de una entidad certificadora o evaluadora de alta calidad, reconocida en el país de origen o a nivel internacional, se procederá a convalidar el título."*

Que consultado el Comité National d'évaluation (CNÉ), entidad evaluadora y acreditadora de la educación superior en FRANCIA, se pudo establecer que la UNIVERSITÉ PARIS 1, se encuentra acreditada.

Que con fundamento en las anteriores consideraciones y después de haber estudiado la documentación presentada, se concluye que es procedente la convalidación solicitada.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO.- Convalidar y reconocer para todos los efectos académicos y legales en Colombia, el título de DIPLOME D' ETUDES APPROFONDIES EN DROIT PUBLIC INTERNE, otorgado el 8 de diciembre de 1999 por la UNIVERSITÉ PARIS 1, Francia, a GUSTAVO VALBUENA QUIÑONES, ciudadano colombiano, identificado con cédula de ciudadanía No.79.779.355, como equivalente al título de MAGÍSTER EN DERECHO PÚBLICO, que otorgan las instituciones de educación superior colombianas de acuerdo con la Ley 30 de 1992.

PARÁGRAFO.- La convalidación que se hace por el presente acto administrativo no exime al profesional beneficiario del cumplimiento de los requisitos exigidos por las normas que regulan el ejercicio de la respectiva profesión.

ARTÍCULO SEGUNDO.- La presente Resolución rige a partir de la fecha de su expedición y contra la misma procede el recurso de reposición, que debe ser presentado dentro de los cinco (5) días hábiles siguientes a su notificación de conformidad con el Código Contencioso Administrativo.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D. C., a los 28 DIC. 2006

LA DIRECTORA DE CALIDAD PARA LA EDUCACIÓN SUPERIOR (E),

ADRIANA MOLINA MANTILLA

43

Industria y Comercio
SUPERINTENDENCIA

Bogotá D.C.
2 de mayo de 2011
5:03:43

LA SECRETARIA GENERAL

HACE CONSTAR

Que revisado los documentos que reposan en la hoja de vida del doctor **GUSTAVO VALBUENA QUIÑONES**, identificado con la cédula de ciudadanía 79.779.355 de Bogotá, registra que prestó sus servicios en esta entidad desde el 17 de Octubre de 2007 hasta el 25 de agosto de 2010 en el cargo de Superintendente 0030-00 asignado a la Superintendencia de Industria y Comercio

Que el doctor Gustavo Valbuena desarrollaba las siguientes funciones:

PROPÓSITO PRINCIPAL

Fijar políticas, adoptar planes generales, dirigir, controlar y velar por el cumplimiento de los objetivos relacionados con la naturaleza y funciones propias de la Superintendencia de Industria y Comercio, desarrollando las políticas generales del gobierno en materia de propiedad industrial, protección del consumidor, protección de la competencia y asuntos jurisdiccionales

DESCRIPCIÓN DE FUNCIONES

1. Fijar las políticas, estrategias y adoptar los planes generales, relacionados con las funciones institucionales, dando cumplimiento a las disposiciones legales vigentes.
2. Velar por el cumplimiento de los objetivos institucionales para el eficiente desempeño de las funciones públicas encomendadas, en concordancia con las disposiciones legales y políticas gubernamentales.
3. Desarrollar las políticas generales de gobierno en relación con propiedad industrial, protección de la competencia, protección al consumidor y asuntos jurisdiccionales, de acuerdo con su naturaleza y funciones propias de la entidad.
4. Expedir los actos administrativos propios de las funciones conferidas por las normas y disposiciones legales.
5. Nombrar, remover y administrar al personal de la Superintendencia de acuerdo con las disposiciones legales vigentes.

Sede Centro: Carrera 13 No. 27-00 Pisos 2, 5, 7 y 10
Sede CAN: Av. Carrera 50 #27-55 int.2 Teléfono. 5870000
Fax. 5870284 Línea 018000910165
Call Center 6513240
Web: www.sic.gov.co e-mail: info@sic.gov.co

Industria y Comercio
SUPERINTENDENCIA

continuación certificación laboral de Gustavo Valbuena Quiñones 02

6. Rendir informes al Presidente de la República y al Ministro de Comercio, Industria y Turismo de conformidad con las normas legales.
7. Autorizar la implementación de procedimientos y trámites administrativos, para el buen funcionamiento de la entidad.
8. Representar al país por delegación del gobierno nacional en reuniones nacionales o internacionales, relacionados con lo temas y objetivos institucionales.
9. Asistir a las reuniones de los consejos, juntas, comités y demás cuerpos en que tenga asiento la entidad o efectuar las delegaciones pertinentes.
10. Implementar el Sistema de Control Interno, de acuerdo con la naturaleza y estructura de la organización, en cumplimiento de las disposiciones legales vigentes.
11. Adelantar las gestiones necesarias para asegurar el oportuno cumplimiento de los planes, programas y proyectos trazados.
12. Adoptar sistemas o canales de información para la ejecución y seguimiento de los planes gubernamentales de que hace parte la institución.
13. Supervisar la implementación del sistema de calidad para asegurar la conveniencia, adecuación y eficacia en la gestión institucional.
14. Las demás que le señalen la Constitución, la ley, los estatutos, normas y disposiciones que determinen la organización de la entidad.

CONTRIBUCIONES INDIVIDUALES (CRITERIOS DE DESEMPEÑO)

1. Las políticas, estrategias y planes generales son fijados dando cumplimiento a las directrices y normas dadas por el Gobierno Nacional.
2. Los objetivos institucionales se desarrollan garantizando el eficiente desempeño de las funciones públicas encomendadas, dando cumplimiento a las disposiciones legales y políticas gubernamentales vigentes.
3. Las políticas generales de gobierno en relación con propiedad industrial, protección de la competencia, protección al consumidor y asuntos jurisdiccionales desarrolladas, están de acuerdo con la naturaleza y las funciones propias de la entidad.
4. Los actos administrativos expedidos cumplen con las normas y disposiciones legales vigentes.
5. El personal de la Superintendencia nombrado, removido y administrado responde a las necesidades de la entidad y está en concordancia con las disposiciones legales vigentes.
6. Los informes al Presidente de la República y Ministro de Comercio, Industria y Turismo son presentados de acuerdo con los requerimientos y disposiciones legales.

Sede Centro: Carrera 13 No. 27-00 Pisos 2, 5, 7 y 10
Sede CAN: Av. Carrera 50 27-35 Int.2 Teléfono 5870205
Fax: 5870284. Línea 018000910165
Cal. Center 6513240
Web: www.sic.gov.co e-mail: info@sic.gov.co

47

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Industria y Comercio
SUPERINTENDENCIA

continuación certificación laboral de Gustavo Valbuena Quiñones 03

7. La autorización de procedimientos y trámites administrativos son realizados dando cumplimiento a las disposiciones legales vigentes.
8. La representación en reuniones nacionales e internacionales se realizan en cumplimiento a las delegaciones conferidas por el Gobierno Nacional.
9. Las reuniones de los consejos, juntas, comités son atendidas adecuada y oportunamente dando cumplimiento a las directrices gubernamentales.
10. El Sistema de Control Interno implementado cuenta con los elementos y controles necesarios de acuerdo con la naturaleza y estructura de la Superintendencia.
11. Los planes, programas y proyectos de la Entidad implementados están de acuerdo con la naturaleza y funciones propias de la institución.
12. Los sistemas o canales de información adoptados disponen de los mecanismos necesarios para la ejecución y seguimiento de los planes gubernamentales.
13. El sistema de calidad es supervisado continuamente con el fin de asegurar la conveniencia, adecuación y eficacia de la gestión institucional.

LIGIA STELLA RODRÍGUEZ HERNÁNDEZ

Elaboró:
Revisó:

49

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

VALBUENA ABOGADOS

CERTIFICA

Que el señor **GUSTAVO VALBUENA QUIÑONES** identificado con la cédula de ciudadanía número 79.779.355 de Bogotá, presta actualmente sus servicios en esta Empresa con contrato a término indefinido, desde el 2 de febrero de 2011 a la fecha, desempeñándose como GERENTE y prestando sus servicios profesionales como abogado consultor y asesor en temas de protección de datos personales.

La presente certificación se expide a los veintiocho (28) de octubre de 2013.

Cordialmente,

GUSTAVO VALBUENA QUIÑONES
Valbuena Abogados

48

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Valbuena ABOGADOS

VALBUENA ABOGADOS

CERTIFICA

Que **MARIA FERNANDA DE LA OSSA ARCHILA** identificada con la cédula de ciudadanía número 57.381.737 de Bogotá, presta actualmente sus servicios en esta Empresa con contrato a término indefinido, desde el 1 de junio de 2012 a la fecha, desempeñándose como ABOGADA ASOCIADA y prestando sus servicios profesionales como asesora jurídica en temas de protección de datos personales.

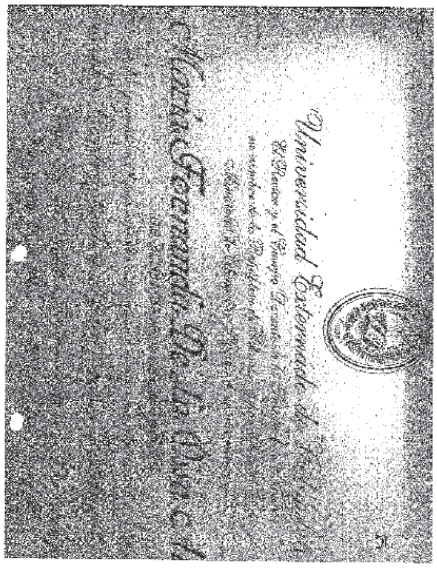
La presente certificación se expide a los veintiocho (28) días del mes de octubre de 2013

Cordialmente,

GUSTAVO VALBUENA QUIÑONES
Valbuena Abogados

50

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA



COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Centros
Internacionales de Idiomas

CERTIFICACIÓN

Yo César Daniel Gómez identificado con cédula de ciudadanía número 1.018.407.963 de Bogotá en mi calidad de Gerente de Producto de la sociedad EF Education First S.A. certifico que la firma VALBUENA ABOGADOS S.A.S durante el periodo comprendido entre los meses de junio y agosto del presente año prestó servicios de asistencia legal y asesoría jurídica en el diseño e implementación de las medidas tendientes a dar cumplimiento a las disposiciones previstas en la Ley 1581 de 2012 y el Decreto reglamentario 1377 de 2013, especialmente en la creación de modelos o formatos para la obtención de la autorización por el tratamiento de datos personales, elaboración y diseño del manual de procedimientos para el tratamiento de datos personales.

El valor de los servicios prestados por la firma VALBUENA ABOGADOS S.A.S, correspondió a la suma de $ 15.000.000 más IVA.

César Daniel Gómez
EF Education First Universidad

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

andiarios

Bogotá, diciembre 4 de 2013

CERTIFICACIÓN

NORA SANÍN POSADA, identificada con cédula de ciudadanía número 41.609.236 en mi calidad de Directora Ejecutiva de la Asociación Colombiana de Editores de Diarios y Medios Informativos **ANDIARIOS**- certifico que la firma **VALBUENA ABOGADOS S.A.S.** durante el periodo comprendido entre el mes de noviembre de 2012 y el mes de julio de 2013 prestó servicios de asesoría legal y asesoría jurídica en el diseño e implementación de las medidas tendientes a dar cumplimiento a las disposiciones previstas en la Ley 1581 de 2012 y el Decreto reglamentario 1377 de 2013, específicamente en la creación de modelos o formatos para la obtención de la autorización por el tratamiento de datos personales, elaboración y diseño del manual de procedimientos para el tratamiento de datos personales y capacitación a los equipos legales de los diarios afiliados.

El valor de los servicios prestados por la firma **VALBUENA ABOGADOS S.A.S.** correspondió a la suma de veintiocho millones de pesos ($ 28.000.000) más IVA.

NORA SANÍN POSADA
Directora Ejecutiva
ANDIARIOS

andiarios

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

mass

CERTIFICACIÓN

EDUARDO SUAREZ identificado con cédula de ciudadanía número 80.420.938b en mi calidad de representante legal de la sociedad **MASS DIGITAL S.A.** certifico que la firma **VALBUENA ABOGADOS S.A.S.** durante el periodo comprendido entre los meses de junio y agosto del presente año prestó servicios de asistencia legal y asesoría jurídica en el diseño e implementación de las medidas tendientes a dar cumplimiento a las disposiciones previstas en la Ley 1581 de 2012 y el Decreto reglamentario 1377 de 2013, especialmente en la creación de modelos o formatos para la obtención de la autorización por el tratamiento de datos personales, elaboración y diseño del manual de procedimientos para el tratamiento de datos personales.

El valor de los servicios prestados por la firma **VALBUENA ABOGADOS S.A.S.** correspondió a la suma de $ 16.500.000 más IVA

EDUARDO SUAREZ
MASS DIGITAL S.A.

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

HYUNDAI

HYUNDAI COLOMBIA AUTOMOTRIZ S.A.
NIT.900.173.557-4

CERTIFICACIÓN

CON DESTINO A

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

PABLO JOSE SALCEDO VISBAL, identificado con cédula de ciudadanía número 12.554.560 de Santa Marta, en mi calidad de Representante Legal de la sociedad **HYUNDAI COLOMBIA AUTOMOTRIZ S.A.**, certifico que la firma **VALBUENA ABOGADOS S.A.S.** NIT. 900.411.302-8, durante el periodo comprendido entre los meses de junio a agosto de 2013 prestó servicios de asistencia legal y asesoría jurídica en el diseño e implementación de las medidas tendientes a dar cumplimiento a las disposiciones previstas en la Ley 1581 de 2012 y el Decreto reglamentario 1377 de 2013, específicamente en la creación de modelos o formatos para la obtención del consentimiento para el tratamiento de datos personales, elaboración y diseño de la política de tratamiento de datos personales, implementación de los mecanismos para la atención de las solicitudes de acceso, rectificación, actualización, supresión de datos o revocatoria del consentimiento dentro de los términos y con observancia del procedimiento establecido en los artículos 14 y 15 de la Ley 1581 de 2012, identificación de estrategias legales para la utilización de bases de datos conformadas antes del Decreto 1377 de 2013 y elaboración del manual de procedimientos para el tratamiento de datos personales, entre otros temas.

Los honorarios profesionales cancelados por el anterior concepto correspondieron a la suma de $11.400.000.

Se firma en Bogotá, a los 10 días del mes de Diciembre de 2013.

Atentamente,

PABLO JOSE SALCEDO VISBAL
Representante Legal
Tel.6760218
Autopista Norte Cl.233 Costado Occidental

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

MinTrabajo

PROSPERIDAD PARA TODOS

El Jefe de la Oficina de Protección al Usuario de la Superintendencia del Subsidio Familiar

Certifica que:

La sociedad **VALBUENA ABOGADOS**, identificada con NIT 900411302-8 participó en el seminario denominado *"V encuentro nacional de atención e interacción con el ciudadano, para jefes de atención al cliente, jefes de subsidio y jefes de planeación de las cajas de compensación familiar"*, el cual se llevó a cabo en la isla de San Andrés desde los días 16 al 18 de octubre de 2013, con la conferencia dictada por el doctor **GUSTAVO VALBUENA QUIÑONES**, identificado con la cédula de ciudadanía 79.779.355 de Bogotá.

Los temas centrales de la conferencia, fueron las leyes de habeas data (Protección de datos) y las obligaciones de las cajas de compensación familiar frente a estas leyes.

Se expide la presente, a solicitud del interesado hoy nueve (9) de diciembre de 2013.

DIEGO ARMANDO GONZALEZ TOLOZA
Jefe Oficina de Protección al Usuario

[illegible]

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

PROSPERIDAD PARA TODOS

La Jefe de la Oficina Asesora Jurídica (E) de la Superintendencia del Subsidio Familiar

Certifica que:

La sociedad **VALBUENA ABOGADOS** identificada con NIT 900411302-8 participó en el seminario denominado *"Actualización normativa para abogados, jefes de subsidio y aportes de las cajas de compensación familiar"* el cual se llevó a cabo en la ciudad de Cartagena los días 28 y 29 de noviembre de 2013, con la conferencia dictada por el doctor **GUSTAVO VALBUENA QUIÑONES**, identificado con la cédula de ciudadanía 79.779.355 de Bogotá.

Los temas centrales de la conferencia, fueron las leyes de habeas data (Protección de datos) y las obligaciones de las cajas de compensación familiar frente a estas leyes.

Se expide la presente, a solicitud del interesado hoy nueve (9) de diciembre de 2013.

LIDA REGINA BULA NARVÁEZ
Jefe Oficina Asesora Jurídica (E)

[illegible]

COMISIÓN PRIMERA
SENADO DE LA REPUBLICA

Comment to Colombia SIC on Privacy and Data Security in the United States

Federal Trade Commission staff welcome this opportunity to provide information regarding the U.S. privacy and data security landscape. We are thankful that the Superintendence of Industry and Commerce (SIC) has consulted with us on these issues, and write to provide a more comprehensive record beyond our discussions.

First, the U.S. Federal Trade Commission ("FTC") has a robust privacy and data security program for U.S. commercial practices that protects consumers worldwide. Second, the landscape of consumer privacy and security protection in the United States has evolved substantially in the last few decades. Many federal and state privacy and security laws have been enacted, and public and private litigation to enforce privacy rights has increased significantly. This note describes the broad scope of U.S. legal protections for consumer privacy and security applicable to commercial data practices in the U.S.

I. The FTC's General Privacy and Data Security Enforcement Program

The FTC is the leading U.S. consumer protection agency focused on commercial sector privacy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. As part of this authority, the FTC can enforce the privacy promises that companies make, including when they participate in self-regulatory programs. The FTC also has authority to enforce more targeted privacy laws that protect certain financial and health information, information about children, and information used to make eligibility decisions about consumers.

The FTC has unparalleled experience in consumer privacy enforcement. The FTC's enforcement actions have addressed unlawful practices in offline and online environments. For example, the FTC has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC, and Snapchat, as well as lesser-known companies. The FTC has sued businesses that allegedly spammed consumers, installed spyware on computers, failed to secure consumers' personal information, deceptively tracked consumers online, violated children's privacy, unlawfully collected information on consumers' mobile devices, and failed to secure Internet-connected devices used to store personal information. The resulting orders have typically provided for ongoing monitoring by the FTC for a period of twenty years, prohibited further law violations, and subjected the businesses to substantial financial penalties for order violations.[1] Importantly, FTC orders do not just protect the individuals who may have complained about a problem; rather, they protect all consumers dealing with the business going forward. In the cross-border context, the FTC has jurisdiction to protect consumers worldwide from practices taking place in the United States.[2]

[1] Any entity that fails to comply with an FTC order is subject to a civil penalty of up to $16,000, with each day of a continuing violation constituting a separate violation. *See* 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

[2] Congress has expressly affirmed the FTC's authority to seek redress for harm abroad caused harm abroad caused from within the United States. *See* 15 U.S.C. § 45(a)(4).

1

The FTC has also pursued numerous policy initiatives aimed at enhancing consumer privacy that inform its enforcement work. The FTC has hosted workshops and issued reports recommending best practices aimed at improving privacy in the mobile ecosystem; increasing transparency of the data broker industry; maximizing the benefits of big data while mitigating its risks, particularly for low-income and underserved consumers; and highlighting the privacy and security implications of Connected cars and the Internet of Things, among other areas.

The FTC also engages in consumer and business education to enhance the impact of its enforcement and policy development initiatives. The FTC has used a variety of tools—publications, online resources, workshops, and social media—to provide educational materials on a wide range of topics, including mobile apps, children's privacy, and data security. Most recently, the Commission launched its "Stick With Security" initiative, providing guidance for businesses drawing on lessons learned from the agency's data security cases, closed investigations, and the experiences of businesses across the country.[3] In addition, the FTC has long been a leader in educating consumers about basic computer security. Our OnGuard Online[4] site and its Spanish language counterpart, Alerta en Linea,[5] have millions of page views per year. Other educational materials can be found in our consumer page[6] and business center.[7]

For the past few years we have prepared detailed reports of our privacy activity. We invite the SIC to access these at the following URLs:

https://www.ftc.gov/reports/privacy-data-security-update-2016

https://www.ftc.gov/reports/privacy-data-security-update-2015

https://www.ftc.gov/reports/privacy-data-security-update-2014

II. Federal and State Protections for Consumer Privacy

Many federal statutes regulate the commercial collection and use of personal information, beyond Section 5 of the FTC Act, including: the Cable Communications Policy Act, the Child Online Privacy Protection Act (COPPA), the Driver's Privacy Protection Act, the Electronic Communications Privacy Act, the Electronic Funds Transfer Act, the Gramm-Leach-Bliley Act, the Right to Financial Privacy Act, the Telephone Consumer Protection Act, and the Video Privacy Protection Act. Many states have analogous laws in these areas as well.

The Fair Credit Reporting Act promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies (CRAs).such as credit bureaus, medical information companies and tenant screening services. Consumers have a right to know when

[3] https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations.
[4] https://www.consumer.ftc.gov/features/feature-0038-onguardonline.
[5] https://www.consumidor.ftc.gov/destacado/destacado-s0038-alerta-en-linea.
[6] https://www.consumer.ftc.gov/.
[7] https://www.ftc.gov/tips-advice/business-center.

information is used against them, to know what is in their file, the right to dispute inaccurate information, and to have inaccurate information deleted.[8] Information in a consumer report cannot be provided to anyone who does not have a purpose specified in the Act. Companies that provide information to consumer reporting agencies also have specific legal obligations, including the duty to investigate disputed information. In addition, users of the information for credit, insurance, or employment purposes must notify the consumer when an adverse action is taken on the basis of such reports. The Fair and Accurate Credit Transactions Act added many provisions to the FCRA primarily relating to record accuracy and identity theft. The FTC has brought over 100 FCRA cases against companies for credit-reporting problems and has collected over $30 million in civil penalties.

The Gramm-Leach-Bliley ("GLB") Act requires financial institutions to send consumers annual privacy notices and allow them to opt out of sharing their information with unaffiliated third parties. It also requires financial institutions to implement reasonable security policies and procedures. Since 2005, the FTC has brought almost 30 cases for violations of the GLB Act.

The Children's Online Privacy Protection Act of 1998 ("COPPA") generally requires websites and apps to obtain parental consent before collecting personal information from children under 13. Since 2000, the FTC has brought over 20 COPPA cases and collected millions of dollars in civil penalties. In 2013, the FTC updated it regulatory rule that implements COPPA to address new developments – such as social networking, smartphone Internet access, and the ability to use geolocation information – that affect children's privacy. (The new rule went into effect July 1, 2013).

Sector-specific federal laws provide for a private right of action in certain circumstances For example, , the Fair Credit Reporting Act provides for a general private right of action for violations of its provisions so long as the action is not being taken against a consumer report user. The Dodd-Frank Act provides for a private right against credit rating agencies that knowingly or recklessly use inaccurate information. The Right to Financial Privacy Act of 1978 provides a private right against government authorities and financial institutions that obtained or disclosed personal information in violation of the Act.

Regarding personal data in the context of the communications sector, private rights of action are afforded by several federal laws. For example, the Electronic Communications Privacy Act (ECPA) provides a private right of action for the unauthorized interception of electronic communications. The Video Privacy Protection Act (VPPA) provides private remedies for unauthorized disclosures of personal information by video tape service providers.

In the last few decades there have been numerous developments at both the federal and state level that provide additional consumer privacy protections.[9] At the federal level, for example, the FTC amended the Children's Online Privacy Protection Rule in 2013 to provide a number of additional protections for additional protections for children's personal information.

[8] https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf
[9] For a more comprehensive summary of the legal protections in the United States, see Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5th ed. 2015).

The FTC also issued two rules implementing the Gramm-Leach-Bliley Act – the Privacy Rule and the Safeguards Rule, which require financial institutions[10] to make disclosures about their information sharing practices and to implement a comprehensive information security program to protect consumer information.[11] Similarly, the Fair and Accurate Credit Transactions Act, enacted in 2003, supplements longstanding U.S. credit laws to establish requirements for the masking, sharing, and disposal of certain sensitive financial data. The FTC promulgated a number of rules under FACTA regarding, among other things, consumers' right to a free annual credit report; secure disposal requirements for consumer report information; consumers' right to opt out of receiving certain offers of credit and insurance; consumers' right to opt out of the use of information provided by an affiliated company to market its products and services; and requirements for financial institutions and creditors to implement identity theft detection and prevention programs.[12] In addition, the Health Insurance Portability and Accountability Act Privacy Rule was revised in 2003 and again in 2013, requiring additional safeguards to protect the privacy of personal health information. Rules protecting consumers from unwanted telemarketing calls, robocalls, and spam have also gone into effect. Congress has also enacted laws requiring certain companies that collect health information to provide consumers with notification in the event of a breach.[13]

States have also been active in passing laws related to privacy and security. Since 2000, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws requiring businesses to notify individuals of security breaches of personal information.[14] At least thirty-two states and Puerto Rico have data disposal laws, establishing requirements for the destruction or disposal of personal information.[15] A number of states also have enacted general data security laws. In addition, California has enacted various privacy laws, including a law requiring companies to have privacy policies and disclose their Do Not Track practices,[16] a "Shine the Light" law requiring greater transparency for data brokers,[17] and a

[10] Financial institutions are defined very broadly under the Gramm-Leach-Bliley Act to include all businesses that are "significantly engaged" in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and professional tax preparers.
[11] Under the Consumer Financial Protection Act of 2010 ("CFPA"), Title X of Pub. L. 111-203, 124 Stat. 1955 (July 21, 2010) (also known as the "Dodd-Frank Wall Street Reform and Consumer Protection Act"), most of the FTC's Gramm-Leach-Bliley Act rulemaking authority was transferred to the Consumer Financial Protection Bureau ("CFPB"). The FTC retains enforcement authority under the Gramm-Leach-Bliley Act as well as rulemaking authority for the Safeguards Rule and limited rulemaking authority under the Privacy Rule with respect to auto dealers.
[12] Under the CFPA, the Commission shares its FCRA enforcement role with the CFPB, but rulemaking authority transferred in large part to the CFPB (with the exception of the Red Flags and Disposal Rules).
[13] *See, e.g.*, American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009); *see also* 16 C.F.R. Part 318.
[14] *See, e.g.*, National Conference of State Legislatures ("NCSL"), *State Security Breach Notification Laws* (Oct. 22, 2015), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[15] NCSL, *Data Disposal Laws* (Jan. 21, 2015), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.
[16] Cal. Bus. & Professional Code §§ 22575-22579.
[17] Cal. Civ. Code §§ 1798.80-1798.84.

law that mandates an "eraser button" allowing minors to request the deletion of certain social media information.[18] Using these laws and other authorities, federal and state governments have levied significant fines against companies that have failed to protect the privacy and security of consumers' personal information.[19]

Private lawsuits have also led to successful judgments and settlements that provide additional privacy and data security protection for consumers.[20] For example, in 2015 Target agreed to pay $10 million as part of a settlement with customers who claimed their personal financial information was compromised by a widespread data breach. Additionally, in 2013, AOL agreed to pay a $5 million settlement to resolve a class action involving alleged inadequate deidentification related to the release of search queries of hundreds of thousands of AOL members. Another federal court approved a $9 million payment by Netflix for allegedly keeping rental history records in violation of the Video Privacy Protection Act of 1988. Federal courts in California approved two separate settlements with Facebook, one for $20 million and another for $9.4 million, involving the company's collection, use, and sharing of its users' personal information. And, in 2008, a California state court approved a $20 million settlement with LensCrafters for unlawful disclosure of consumers' medical information.

State contract law may also provide an avenue for private relief under several scenarios:

- Express Contractual Obligations: Data subjects may bring a private action against a company with which they have entered into a contractual agreement governing the use of their data. For example, online agreements, such as "terms of use" agreements, can create contractual obligations under state law through express terms governing data use and protection. A data subject may bring a contractual claim if (1) a company violated the *express terms* in an agreement and; (2) those terms were *validly accepted by the subject*. To prove valid acceptance of an agreement, the data subject must show affirmative manifestation of assent. *See In re Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d 1197, 1206 (N.D. Cal. 2014); *Fero v. Excellus Health Plan, Inc.*, No. 6:15–CV–06569 EAW, 2017 WL 713660 at *3 (W.D.N.Y. Feb. 2, 2017).

- Implied Contractual Obligations: A data subject may also bring a contractual claim based upon an implied contract created through the use of a method of payment that imparts personal information. The use of certain methods of payment, such as credit or debit cards, creates an implied contractual agreement that the data controller will use the data for a specific purpose and take reasonable steps to secure the data. If the controller fails to do so, the data subject has a contractual claim. *See In re Hannaford Bros. Customer Data Sec. Breach Litig.*, 613 F. Supp.2d 108, 118 (D. Me. 2009), aff'd, 659 F.3d 151, 158-59 (1st Cir. 2011).

[18] Cal. Bus. & Professional Code § 22580 *et seq.*
[19] *See* Jay Cline, *U.S. Takes the Gold in Dishing Out Privacy Fines*, Computerworld (Feb. 17, 2014), *available at* http://www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=17&pageNumber=1.
[20] *Id.*

- Intended Beneficiaries: In addition, data subject may also enforce a contract between the company receiving the data and contractor processing the data, provided that the data subject is an *intended beneficiary* or belongs to a class of intended beneficiaries. In order to establish intended beneficiary status, a plaintiff must show: (1) that the contracting parties have clearly intended to confer a benefit; and (2) that "clear intent" is manifested in the contract. For example, passport applicants successfully filed suit against defendant CGI Federal for failing to adequately safeguard their personal information after it was stolen and misused. The court reasoned that the State Department had transferred the applicants' data to CGI Federal with a contract provision that specifically required CGI to protect plaintiffs' personal information, thereby intending to confer a benefit on plaintiffs. *See Sovereign Bank v. B.J.'s Wholesale Club, Inc.*, 533 F.3d 162, 170 (3d Cir. 2008).

In sum, as the discussion above illustrates, the United States provides significant legal protection for consumer privacy and data security.

For further information regarding these issues, please contact Hugh Stevenson, hstevenson@ftc.gov, Michael Panzera, mpanzera@ftc.gov, or Guilherme Roschke groschke@ftc.gov, at the FTC's Office of International Affairs.

Siendo las 12:56 p.m., la Presidencia levanta la sesión y convoca para el día miércoles 20 de septiembre de 2017, a partir de las 10:00 a.m., en el salón Guillermo Valencia del Capitolio Nacional.

PRESIDENTE,

ROOSVELT RODRIGUEZ RENGIFO

VICEPRESIDENTE,

HORACIO SERPA URIBE

SECRETARIO GENERAL,

GUILLERMO LEON GIRALDO GIL

IMPRENTA NACIONAL DE COLOMBIA - 2017