Guía GECTI para la implementación del principio de responsabilidad demostrada –*accountability*– en las transferencias internacionales de datos personales

Recomendaciones para los países latinoamericanos

Nelson Remolina Angarita
Luisa Fernanda Álvarez Zuluaga

Universidad de los Andes
Colombia

GECTI

Observatorio Ciro Angarita Barón
sobre la protección de datos personales

Junio del 2018

© Universidad de los Andes
Facultad de Derecho
Carrera 1 n.º 18A-10, Edificio RGC, piso 2
Bogotá, D. C., Colombia
Teléfono: 339 49 49
https://derecho.uniandes.edu.co

ISBN: 978-958-774-696-9

ISBN *e-book*: 978-958-774-697-6

Cómo citar: Remolina Angarita, Nelson. Álvarez Zuluaga, Luisa Fernanda. (2018). *Guía GECTI para la implementación del principio de responsabilidad demostrada* –accountability– *en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos*. Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI, 1-58.

Contacto: Nelson Remolina Angarita
nremolin@uniandes.edu.co

Diseño editorial y diagramación: Karina Betancur Olmos

Universidad de los Andes | Vigilada Mineducación
Reconocimiento como universidad: Decreto 1297 del 30 de mayo de 1964
Reconocimiento de personería jurídica: Resolución 28 del 23 de febrero de 1949, Minjusticia
Acreditación institucional de alta calidad, 10 años: Resolución 582 del 9 de enero del 2015, Mineducación

Contenido

¿Quiénes somos?

El Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) fue creado el 5 de octubre del 2001 en la Facultad de Derecho de la Universidad de los Andes (Bogotá, Colombia) con el fin de fomentar el trabajo multidisciplinario y establecer un puente entre la Universidad y la sociedad para procurar reflexiones y acciones en materia de la internet, la sociedad de la información y temas convergentes.

La misión del GECTI[1] consiste en hacer un aporte académico independiente sobre diferentes aspectos del ciberespacio, la economía digital y la realidad socio-tecnológica contemporánea, así como realizar investigaciones, consultorías, publicaciones y programas académicos de alto nivel especializados en derecho y tecnología.

El Observatorio Ciro Angarita Barón sobre la protección de datos personales en Colombia[2], por su parte, fue fundado el 17 de enero del 2008 en la Facultad de Derecho de la Universidad de los Andes (Bogotá, Colombia) y representa un espacio académico de reflexión sobre la protección de los derechos de las personas cuando sus datos son recolectados, almacenados o utilizados por terceros.

1 La página *web* del GECTI es: https://gecti.uniandes.edu.co.

2 La página *web* del Observatorio es: https://habeasdatacolombia.uniandes.edu.co.

Introducción

El tratamiento de datos personales se ha caracterizado por su internacionalidad, gracias al carácter transfronterizo de buena parte de su recolección, uso y circulación. La economía digital, el comercio internacional, el comercio electrónico y muchas otras actividades requieren la circulación internacional de datos personales. En adición a la libre circulación de mercancías, personas y capitales, la exportación e importación de datos personales es un insumo importante para el funcionamiento del mercado y el éxito de varios negocios.

El principio de *accountability* —responsabilidad demostrada— ha cobrado gran importancia en el tratamiento de datos personales, ya que su real y debida implementación no sólo redundará en beneficio de la protección de los derechos de titulares de los datos personales sino que beneficiará muy positivamente a las organizaciones porque les permitirá maximizar el uso inteligente de la información, aumentar su nivel de competitividad y consolidar su buena reputación empresarial o institucional.

Es crucial que los directivos y directivas de las organizaciones sean proactivos respecto del tratamiento de la información, de manera que por iniciativa propia se anticipen a los eventuales problemas y adopten medidas estratégicas capaces de neutralizarlos o que les permitan a las organizaciones explotar la información dentro de un escenario competitivo, innovador y respetuoso de los derechos humanos.

Con miras a contribuir a la consolidación del debido tratamiento de datos que son transferidos internacionalmente, queremos que esta guía sea un referente útil, cuyo objetivo señalamos a continuación.

Objetivo de esta guía

El propósito de esta guía consiste en presentar algunas recomendaciones a quienes envían datos personales a otros países. Como tal, proponemos algunas orientaciones para que la circulación transfronteriza de datos personales se realice respetando los derechos de los titulares de los datos y protegiendo los intereses de los responsables o encargados del tratamiento de los mismos.

La guía está orientada para que sea utilizada en los países latinoamericanos y busca desarrollar aspectos que aún no han sido incluidos expresamente en guías de *accountability* como la de la República de Colombia, que por ahora es la única que existe en Latinoamérica.

Por lo tanto, esperamos que este documento sea tenido en cuenta para la elaboración de futuras guías de *accountability* por otras autoridades de protección de datos de países latinoamericanos.

Este texto no es un concepto legal ni constituye asesoría jurídica. Las recomendaciones deben ajustarse teniendo en cuenta las particularidades de cada organización.

I. Antecedentes e importancia

• El tratamiento de datos personales como un asunto global y una actividad cotidiana en el ciberespacio

Vivimos en un planeta fraccionado geográficamente pero fusionado tecnológicamente en donde la información es el principal bien que circula a través de una infraestructura tecnológica global hiperconectada que sirve de soporte del ciberespacio[3]. Por eso, el tratamiento[4] de datos personales (en adelante, TDP) cada día es más transfronterizo y global.

Como es sabido, el uso de bases de datos es una actividad cotidiana y crucial para el Estado, las empresas y los particulares que requieren dicha información para tomar e implementar decisiones de diversa naturaleza. Igualmente, los datos personales representan, en ciertos casos, el principal activo de empresas que se dedican a analizarlos, venderlos, alquilarlos y cederlos. En otros casos se utilizan para tomar decisiones sobre las personas o para fijar políticas públicas, económicas, de riesgo, de mercadeo, entre otras.

3 Aunque se dice que el ciberespacio es un escenario artificial creado por medios tecnológicos, no debe perderse de vista que en el ciberespacio interactúan personas reales de diferente nacionalidad y domiciliadas en prácticamente cualquier parte de nuestro planeta cuyas comunicaciones y actividades traspasan el espacio geográfico de todos los países del mundo.

4 A efectos del presente documento, las expresiones "tratar" o "tratamiento" se entenderán como cualquier operación o conjunto de operaciones aplicadas a datos personales, como la recolección, el registro, la organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a aquellos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

Las tecnologías de la información y la comunicación (TIC), por su parte, han contribuido a la "datificación" de la sociedad contemporánea y a la consolidación del dato personal como el bien más apetecido de la economía digital. La datificación obedece a muchas razones pero, principalmente, a que los datos personales son la moneda de la economía digital o la moneda de oro del siglo XXI.

El tratamiento de datos personales es uno de los temas que en los últimos cincuenta años han llamado la atención de los reguladores y las organizaciones. Inicialmente fue poco reglamentado, pero en la última década se ha venido presentado una eclosión mundial de normas sectoriales y generales, aunada a una revisión de las primeras iniciativas regulatorias, así como múltiples conferencias a todo nivel que ponen de presente la indiscutible relevancia social y económica del tratamiento de la información de las personas.

El derecho a la protección de datos personales que se conoce hoy en día ha tenido importantes cambios desde sus primeras manifestaciones en la regulación de la década de los setenta y los documentos emitidos posteriormente. A los motivos iniciales que dieron origen a su reglamentación se sumaron otros factores que han hecho que los retos de la protección de este derecho sean diferentes de los inicialmente previstos.

La regulación sobre el derecho al debido tratamiento de los datos personales no solo tiene en cuenta los intereses del titular del dato sino que reconoce que esa información es necesaria para realizar muchas actividades lícitas, legítimas y de interés general o particular, según el caso. Por eso la normatividad no se opone al tratamiento, sino que exige que esté rodeado de garantías mínimas para asegurar el correcto tratamiento de la información sobre las personas. En suma, la regulación no se opone al uso de los datos sino al eventual abuso de éstos, para que no se convierta en un hecho generador de la amenaza o vulneración de derechos humanos de los titulares de los datos.

Varios países cuentan con regulaciones generales y sectoriales así como jurisprudencia sobre tratamiento de datos personales. Aunque se ha procurado armonizar internacionalmente los principales aspectos sobre el tratamiento de datos personales, en la práctica cada estado expide normas que parcialmente siguen dichos documentos internacionales pero que al mismo tiempo están impregnadas de las particularidades sociales, políticas, culturales y jurídicas de cada uno. Además, cada sistema jurídico nacional cuenta con diversas herramientas jurídicas (constitucionales, administrativas, judiciales, entre otras) para proteger el derecho al debido tratamiento de datos personales.

Sería pretencioso intentar abordar en detalle todo lo atinente al tratamiento de datos personales desde la perspectiva del derecho comparado. No obstante, es relevante señalar que a partir de los años ochenta se ha realizado una labor muy importante de armonización internacional del derecho de la protección de datos personales[5].

Las respuestas normativas al tratamiento de datos personales se caracterizan, entre otras razones, por tener un enfoque internacional y ser armonizadas. Por eso, la recolección, el almacenamiento, el uso, la circulación y demás actividades sobre los datos personales han sido objeto de una labor de armonización internacional en regulación con miras a lograr un consenso jurídico coherente sobre temas cardinales de dicha materia[6]. En ese sentido, diferentes organizaciones internacionales, redes

5 Respecto del panorama internacional de la protección de datos personales véase Remolina Angarita, Nelson: *Data protection*: panorama nacional e internacional, en *Internet, comercio electrónico y telecomunicaciones*, pp. 99-172, Bogotá: Legis, 2002.

6 En la citada declaración UE-EEUU sobre comercio electrónico se puntualizó que "el papel de los gobiernos es proporcionar un marco legal claro y consistente, promover un entorno competitivo en el que el comercio electrónico pueda florecer y asegurar la protección adecuada de objetivos de interés público como la intimidad, los derechos de propiedad intelectual, la prevención del fraude, la protección del consumidor y la seguridad nacional".

especializadas o grupos de autoridades han publicado documentos contentivos de las reglas que deben observarse en el tratamiento de datos personales, dentro de las cuales se encuentran varios principios que evocan los grandes mensajes o propósitos que se deben materializar para lograr que los derechos de las personas no sean amenazados o vulnerados por la indebida recolección, almacenamiento, uso o circulación de dicha información.

En la tabla n.º 1 (siguiente página) resumimos los principales documentos sobre tratamiento de datos personales emitidos por diferentes organizaciones.

• Relevancia constitucional de la protección de datos en los países latinoamericanos

La protección de datos personales es un asunto de relevancia constitucional en el escenario latinoamericano[7]. Lo anterior se corrobora en un reporte realizado por Nelson Remolina Angarita[8] titulado "Latin America and Protection of Personal Data: Facts and Figures (1985-2014)", en el cual se pone de presente el estado del arte de la regulación sobre datos personales en los siguientes veinte países de América Latina: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela.

7 Sobre el *habeas data* en Latinoamérica, véase Puccinelli, Oscar. 1999. *El* habeas data *en Indoiberoamérica*, Bogotá: Temis.

8 Cfr. Remolina, Nelson. Latin America and Protection of Personal Data: Facts and Figures (1985-2014) (March 20, 2014). Disponible en SSRN: https://ssrn.com/abstract=241209 o en http://dx.doi.org/10.2139/ssrn.241209. El texto fue inicialmente publicado por el Observatorio Ciro Angarita Barón sobre la protección de datos personales en Colombia.

Tabla n.º 1. Principales organizaciones internacionales que
han emitido documentos sobre tratamiento de datos personales

Organización	Principales documentos
Red Iberoamericana de Protección de Datos (RIPD)	Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017)
Unión Europea (UE)	1. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril del 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); 2. Protocolos adicionales al Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y relativo a la transferencia de datos (2001 y 2018); 3. Carta de los Derechos Fundamentales de la Unión Europea (2000); 4. Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (1981)
Organización de Estados Americanos (OEA)	Principios de la OEA sobre la privacidad y la protección de datos personales con anotaciones (2015)
Organización para la Cooperación y el Desarrollo Económicos (OCDE)	Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales (2013, 1980)
Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP)	Estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal –Resolución de Madrid– (2009)
Foro de Cooperación Económica Asia Pacífico (APEC)	Marco de privacidad APEC (2004) APEC Cross Border Privacy Rules (CBPR) APEC Cross Border Privacy Enforcement Arrangement (CPEA)
Organización de las Naciones Unidas (ONU)	Resolución 45/95 del 14 de diciembre de 1990. Principios rectores para la reglamentación de los ficheros computadorizados de datos personales

Fuente: elaboración de Nelson Remolina Angarita©.

Respecto de lo que dicen los textos de las constituciones de dichos países se concluyó lo siguiente:

- El 70% de los países latinoamericanos incorpora en su Constitución disposiciones explícitas referentes a aspectos relacionados con la protección de datos personales.
- El 100% de las disposiciones constitucionales consagra el derecho de acceso de la persona a conocer sus datos y el 92,85% menciona explícitamente el dato personal o la información personal.
- El 85,71% establece el derecho del titular del dato a solicitar la rectificación o la corrección de la información errónea, mientras que el 64,28% le confiere el derecho constitucional de solicitar la supresión, eliminación, destrucción o cancelación del dato.
- El 64,28% considera la actualización de la información un derecho del titular del dato personal.
- El 57,14% establece el *habeas data* y el 7,14% la acción de amparo y acción de protección de privacidad.
- El 50% consagra el derecho a conocer la finalidad del tratamiento de los datos y el 21,42% el derecho a saber el uso que se les está dando a estos.
- El 28,57% erige como derecho constitucional el exigir la confidencialidad sobre los datos personales.
- El 14,28% de las constituciones analizadas otorgan expresamente rango constitucional a la protección de los datos personales.

– Panamá (2004), Ecuador (2008) y México (2009) consagran explícitamente el derecho a la "protección" de la "información personal" y a la "protección de los datos personales".

– República Dominicana (2010) es el único país que contiene un plexo de principios constitucionales (calidad, licitud, lealtad, seguridad y finalidad) que deben regir el tratamiento de datos personales.

– Las constituciones de Panamá y Ecuador exigen que los datos personales se recolecten con el consentimiento del titular del dato.

Recientemente, el Senado de Chile aprobó un proyecto de reforma constitucional mediante el cual se garantiza la protección de los datos personales y se ordena que el tratamiento y la protección de esa información se efectuarán como lo indique la ley[9].

En cuanto a las leyes de dichos países, se concluyó que el 100% de ellos cuenta con normas sectoriales —sobre distintos temas, como historias clínicas y censos de la población— y el 50% cuenta con normas generales.

Al ser un derecho de naturaleza constitucional se requiere especial cuidado y diligencia en el tratamiento de esta información, razón por la cual al responsable del tratamiento se le impone un alto grado de responsabilidad jurídica en esta materia.

9 Cfr. Senado de Chile. Departamento de Prensa. Boletín n.º 9384-07: Protección a los datos personales como derecho constitucional será una realidad. Disponible en http://www.senado.cl/proteccion-a-los-datos-personales-como-derecho-constitucional-sera-una/prontus_senado/2018-05-15/181511.html#vtxt_cuerpo_T0.

• Buen gobierno de datos personales, responsabilidad digital empresarial y responsabilidad jurídica de los directivos de una organización

Es indiscutible la importancia estratégica y económica de los sistemas de información, especialmente de aquellos que contienen datos de personas. De hecho, muchos modelos de negocios se basan en el uso de la información personal. En ese sentido, un artículo publicado en la *Harvard Business Review*, por ejemplo, establece que los nuevos patrones de innovación y las nuevas fronteras de la *generación de valor* están en el tratamiento de la información[10].

También se ha afirmado que las empresas que tengan un correcto tratamiento de los datos personales serán las que lideren la *economía digital* del mañana[11]. En línea con lo anterior, también se ha insistido en que "el debido cuidado en el tratamiento de la información, que asiste a la *responsabilidad digital empresarial*, se convertirá en una norma de facto para las empresas de este siglo que aspiran a ser protagonistas en su sector de negocio"[12].

10 Cfr. Parmar, R., Mackenzie, I., Cohn, D. y Gann, D. (2014) The new patterns of innovation. Harvard Business Review. January-February. Disponible en: https://hbr.org/2014/01/the-new-patterns-of-innovation Citado por Jeimy Cano (2014) en Presiones emergentes sobre la privacidad de la información, en http://insecurityit.blogspot.com.co/2014/05/presiones-emergentes-sobre-la.html.

11 Cfr. Accenture (2016). Guarding and growing personal data value Organizations that demonstrate responsibility in the way they handle personal data today will lead the digital economy of tomorrow. Enero. En https://www.accenture.com/us-en/insight-guarding-growing-personal-data-value.aspx.

12 Cfr. Cano Martínez, Jeimy. 2016. ¿Eres una empresa digitalmente responsable? Enero 20. En https://www.linkedin.com/pulse/eres-una-empresa-digitalmente-responsable-jeimy-cano-ph-d-cfe.

Todo lo anterior ha puesto de presente la necesidad de diseñar e implementar adecuadas estrategias de "buen gobierno y gestión" de la información. Con ellas se pretende: 1. fijar caminos o políticas institucionales a seguir frente a escenarios presentes o futuros de la organización; 2. alcanzar resultados verificables respecto del tratamiento de la información y 3. proteger y maximizar el uso inteligente de la información.

Los gerentes, los miembros de juntas directivas y demás directivos de una organización no sólo tienen una responsabilidad social y ética sino que, según la regulación de cada país, tienen un alto nivel de responsabilidad jurídica. En Colombia, por ejemplo, el representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y quienes de acuerdo con los estatutos ejerzan o detenten esas funciones "deben obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios"[13]. Además, todos ellos jurídicamente responden de manera solidaria e ilimitada por los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros[14]. Se suma a lo anterior, que existe una presunción legal de responsabilidad sobre los gerentes o directivos en los casos de "incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos". Esto último pone de presente el alto grado de nivel de profesionalismo, ética y diligencia que deben observar y demostrar los directivos de una organización en todo lo atinente a, entre otros, el tratamiento de datos personales.

La responsabilidad digital y el buen gobierno de datos es algo que no sólo debe observarse cuando se tratan datos dentro de un territorio sino cuando estos se exporten. Este tema será objeto de reflexiones en las siguientes líneas.

13 República de Colombia. Ley 222 de 1995, artículo 23.

14 Ibídem, artículo 24.

- "Paraísos informáticos" en el tratamiento de datos personales e "internet de las empresas" (*Internet of corporations*)

Muchos países del mundo carecen de normas sobre tratamiento de datos, lo cual significa que en esas partes del planeta no hay certeza sobre la forma de proteger los derechos de los titulares de los datos o simplemente no se protege a las personas frente al tratamiento indebido de los datos personales. En la nota explicativa[15] del Convenio 108 del Consejo de Europa[16] del 28 de enero de 1981, se reconoció la existencia de países que no tienen leyes de protección de datos o que las tienen pero con niveles bajos de protección, denominados "paraísos informáticos" (*data havens*) en donde la protección de los derechos de los titulares de los datos es débil o inexistente.

Palazzi, en referencia al artículo 25 de la Directiva 95/46/CE, comenta que la finalidad de esta es "evitar la creación de paraísos informáticos (*data havens*), es decir, jurisdicciones donde la carencia de leyes de protección de datos, las transforme en sitios atractivos para realizar tratamientos de datos personales que pueden ser violatorios de otras leyes de privacidad"[17]. Los "paraísos informáticos" no sólo comprenden países sin regulación sobre tratamiento de datos personales sino que también cobija otros temas, como los delitos informáticos. Para la ONU, por ejemplo,

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

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

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

los "paraísos informáticos" son "estados que no dan prioridad a la reducción o prevención del uso ilícito de las redes de computadoras, o donde no se han elaborado leyes de procedimiento eficaces"[18].

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

Aunque la citada expresión —"paraísos informáticos"— usualmente se vincula a los países, también se puede replicar a empresas que no son serias con la protección de los datos personales de sus clientes o a las que no les interesa nada diferente de lucrarse de la información de sus clientes sin garantizar un debido tratamiento de los datos de las personas y la protección de los derechos constitucionales de sus clientes.

No obstante lo anterior, los riesgos para las empresas y las personas no sólo surgen en los paraísos informáticos sino en países con niveles adecuados de protección porque la extraterritorialidad de estas actividades prácticamente hacen que los responsables del tratamiento (empresas, entidades públicas) y los titulares del dato (ciudadanos) pierdan el control de la información y se sometan a leyes y decisiones de autoridades, organizaciones o empresas de otros países.

18 Cfr. Organización de las Naciones Unidas. 2000. Delitos relacionados con las redes informáticas. Documento A/CONF.187/10 sobre antecedentes para el curso práctico sobre delitos relacionados con las redes informáticas. En Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. Viena: ONU, p. 3.

Respecto de algunas empresas, no debe perderse de vista que tienen más poder que los estados y sus autoridades. Ellas, mediante sus notas legales y políticas corporativas, regulan los derechos de trillones de personas en la internet. En efecto, tal y como se ha puesto de presente, la "internet de las empresas" sintetiza, en gran parte, lo que ha ocurrido con la regulación de la internet.

La "internet de las empresas" ha fijado el destino de la internet y de sus usuarios porque ha sido hiperregulada por las empresas, que utilizan sus "notas legales" o sus "términos y condiciones" para establecer las reglas que regirán el destino de millones de personas ubicadas en muchas partes del mundo. La "internet de las empresas"[19] se refiere a las normas que los empresarios han creado para realizar negocios o prestar servicios en la internet. Se trata de las pautas que los empresarios consideran sensatas bajo su modelo de negocios para ganar utilidades. En últimas, la "internet de las empresas" es la internet que las empresas desean para ganar dinero. Podríamos denominar a estas regulaciones las "leyes empresariales", las cuales, recalcamos, en la práctica tienen más incidencia y aplicación transfronteriza que cualquier ley local de un estado.

• Transferencias internacionales de datos personales

Las transferencias internacionales fueron uno de los principales motivos que generaron la regulación sobre tratamiento de datos personales. En efecto, el 23 de septiembre de 1980 la Organización para la Cooperación y el Desarrollo Económicos (OCDE)

19 Sobre la internet de las empresas, véase Remolina Angarita, Nelson. (2016) "Internet de las empresas" ["Internet of Corporations" -IoC-]: una explicación de lo que pasa en internet y del futuro de la protección de los derechos humanos en el ciberespacio (parte 1). Universidad de los Andes. Publicado en: https://habeasdatacolombia.uniandes.edu.co/?p=2222.

expidió unas directrices que desde su encabezado fueron explícitas en reconocer dichas transferencias —junto con la protección de la intimidad— como las principales razones que motivaron la redacción de las recomendaciones de dicha organización[20].

Las directrices declaran la necesidad de proteger el derecho de la intimidad[21] para facilitar la transferencia internacional de datos con miras a favorecer, entre otros, el desarrollo social y económico[22] y los negocios que requieren tratar este tipo de información. El documento reconoce explícitamente que "los países miembros tienen un interés común en proteger la intimidad y las libertades individuales, y en reconciliar los valores fundamentales en oposición, tales como la intimidad y la libre circulación de información"[23].

Existe pluralismo terminológico para referirse a las transferencias y a las transmisiones internacionales de datos. Así, por ejemplo, en varios documentos internacionales se les denomina de la siguiente manera:

Circulación transfronteriza de datos personales (OCDE, 1980), "Flujos transfronterizos de datos de carácter personal" (Convenio 108 de 1981), "Transferencia de datos

20 Cfr. Organización para la Cooperación y el Desarrollo Económicos (OCDE). 1980. Recomendación del Consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales.

21 Dentro de los reconocimiento de las directrices se establece que "la legislación nacional relativa a la protección de la intimidad y de la circulación transfronteriza de datos personales puede obstaculizar tal circulación transfronteriza"; por eso dentro de las recomendaciones la OCDE solicita a los estados miembros que "procuren retirar o evitar la creación, en aras de la protección de la intimidad, los obstáculos injustificados a la circulación transfronteriza de datos personales".

22 Cfr. en la parte de reconocimientos de las directrices se indica que "la circulación transfronteriza de datos personales contribuye al desarrollo económico y social".

23 Cfr. la sección de reconocimientos de las directrices de la OCDE, 1980, ob. cit.

personales a países terceros" (Directiva 95/46); "Transferencia de datos a destinatarios no sometidos a las partes del Convenio" (Protocolo adicional del 2001 al convenio 108); "Flujo de datos a través de las fronteras" (Resolución 45/95 de 1990 de la ONU); "Transferencia a otra persona u organización internacional" (APEC, 2004), "Transferencia internacional de datos" (APEC, 2013), "Transferencias internacionales" (Resolución de Madrid del 2009), "Flujo transfronterizo de datos" (OEA, 2015), "Transferencias de datos personales a terceros países u organizaciones internacionales" (Reglamento UE 2016/679) y "Transferencias internacionales de datos personales" (Red Iberoamericana de Protección de Datos, 2017).

Al margen de su denominación, las transferencias internacionales se refieren al envío de datos personales desde un país por un responsable o encargado de datos a otro responsable o encargado de ubicarlo en otro u otros países. En últimas, los datos personales son remitidos o exportados desde un país a empresas y organizaciones ubicadas en un territorio diferente al del país de envío. Se trata de un proceso de exportación de datos personales.

No obstante, según la regulación de cada país, las expresiones para referirse a este fenómeno difieren cuando se exporta de un responsable a otro responsable (caso en el cual se denomina *transferencia*) o cuando se envían datos de un responsable a un encargado (situación que se denomina *transmisión*). A continuación nos referiremos brevemente a este último.

• Transmisiones internacionales de datos

La transmisión de datos consiste en la entrega o el envío de datos personales por un responsable al encargado del tratamiento de ellos. Las transmisiones pueden ser nacionales o internacionales. Las primeras tienen lugar cuando la remisión de los

datos al encargado no implica que los datos salgan de la República de Colombia, y las segundas ocurren cuando los datos enviados al encargado efectivamente salen fuera del territorio colombiano.

La transmisión no fue prevista en la Ley 1581 del 2012, y en otros países, como México, se le denomina "remisión"[24]. Con ella el regulador quiso diferenciar el suministro de datos a alguien que actúa en nombre y por cuenta del responsable del tratamiento de la entrega de datos y la entrega a otra persona que obra en nombre propio. En la transmisión al final del día el tratamiento sigue bajo la competencia del responsable, quien, por cuestiones prácticas o necesidad entrega los datos al encargado para que realice el tratamiento por su cuenta y bajo sus instrucciones.

El contrato de transmisión internacional de datos personales, por su parte, es el acuerdo de voluntades mediante el cual el responsable y el encargado establecen las condiciones y obligaciones que asumirá el encargado para realizar el tratamiento de datos en nombre del responsable. El artículo 24 del Decreto 1377 del 2013 —incorporado en el Decreto 1074 del 2015— establece que las transmisiones internacionales "no requerirán ser informadas al titular ni contar con su consentimiento cuando exista un contrato" de transmisión entre el responsable y el encargado. Dicho contrato está regulado en el artículo 25 de dicho decreto, del cual se deriva lo siguiente:

En primer lugar, se recalca que el encargado realizará el tratamiento bajo la responsabilidad y el control del responsable del tratamiento[25]. Por eso, en el contrato se debe

24 En efecto, en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares del 2011 de los Estados Unidos Mexicanos se define "remisión" como la "comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio" (numeral IX del artículo 2º).

25 Esto también se establece en el considerando número 15 de la Decisión 2010/78/CE en los siguientes términos: "El importador de datos tratará los datos personales transferidos sólo en nombre del exportador de

definir el alcance del tratamiento, sus finalidades y las obligaciones del encargado respecto del titular del dato y el responsable. En segundo lugar, se precisa que las obligaciones fijadas en la Política de Tratamiento de Información (PTI) del responsable deben ser cumplidas por el encargado observado la mencionada PTI. En otras palabras, la PTI del responsable hace parte del contrato y debe ser observada por el encargado.

En tercer lugar, la finalidad del tratamiento debe ser la autorizada por el titular del dato o por la ley. El responsable debe asegurarse de estar legitimado para tratar los datos y de encomendar al encargado realizar actividades autorizadas por el titular o permitidas por la ley. Se recalca que el uso de la información no es ilimitado sino que depende de los supuestos mencionados (autorización o ley). Finalmente, y en adición a lo anterior, en el contrato es obligatorio incluir, por lo menos, estas obligaciones a cargo del encargado, según lo dispuesto por el citado artículo 25:

> […] las siguientes obligaciones en cabeza del respectivo encargado: 1. Dar tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan; 2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales y 3. Guardar confidencialidad respecto del tratamiento de los datos personales.

---

datos y de conformidad con las instrucciones que reciba y las obligaciones impuestas en las cláusulas. En particular, el importador de datos no revelará los datos personales a terceros sin el consentimiento por escrito previo del exportador de datos. El exportador de datos dará instrucciones al importador de datos durante la prestación de los servicios de tratamiento de los datos para que se lleve a cabo de conformidad con sus instrucciones, la legislación de protección de datos aplicable y las obligaciones impuestas en las cláusulas".

• Riesgos que genera la transferencia internacional de datos a las empresas, organizaciones o entidades públicas

La transferencia de datos no sólo pone en riesgo el respeto y efectividad de las personas sino los intereses y principales activos de las organizaciones. A continuación destacamos los principales riesgos para unos y otros:

Eventualmente puede sucederle lo siguiente a una empresa, organización o entidad pública:

- Ser catalogada como un "paraíso informático" por exportar datos sin respetar los derechos de los titulares de los datos.
- Pérdida de control de la información. Si para el empresario es valiosa la información, pues lo mínimo que debe hacer es cuidarla, protegerla y usarla dentro de un escenario leal, legal y respetuoso de los derechos de sus clientes.
- Afectación de la reputación de la organización por enviar datos a "paraísos informáticos", a empresas de dudoso compromiso con la protección de datos o por no hacer todo lo posible para proteger debidamente los datos de sus clientes, ciudadanos o amigos.
- Acceso no autorizado a la información.
- Uso indebido de la información.
- Manipulación o destrucción de la información.
- Reenvío de la información de países con nivel adecuado a otros sin dicho nivel o a paraísos informáticos.

– Que su información sea reenviada indefinidamente de un país a otro(s) sin ningún control o garantías (transferencias ulteriores de datos).

• Riesgos que crea la transferencia internacional de datos a las personas (titulares de los datos) y sus derechos humanos

Enviar datos personales fuera del país pone en mayor riesgo la posibilidad de garantizar la plena observancia del derecho a la protección de datos personales y expone a los ciudadanos de un país a otros riesgos de tipo jurídico y político por el mero hecho de que su información salga de su país.

Con el envío de los datos de una persona a un país, normalmente sucede lo siguiente:

– Que sus datos sean enviados a países o empresas que en la práctica son paraísos informáticos porque la protección de los datos personales es débil o inexistente.

– Inaplicabilidad de la ley de protección del país en donde se tratan los datos personales que van a ser exportados a otro país.

– Sometimiento de los ciudadanos de un país a leyes y jueces extranjeros, así como a las políticas corporativas de empresas y organizaciones de otros países.

– Ausencia de garantía plena del derecho fundamental a la protección de datos personales.

– Pérdida de control de la información por el ciudadano.

– Sumisión de los ciudadanos de un país a las decisiones de los gobiernos, autoridades o empresas de otros países.

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

– Imposición de cargas adicionales a los ciudadanos de un país para el ejercicio de sus derechos en otros países.

• Objetivos de las reglas sobre transferencias internacionales de datos personales

Las regulaciones sobre transferencia internacional de datos[26] o "flujo transfronterizo de datos"[27] procuran garantizar que el nivel de protección de los datos personales de los ciudadanos de un país no disminuya cuando estos deben ser exportados o transferidos a otro u otros países. Esta regla se conoce como el principio de continuidad de la protección de datos, el cual se fundamenta en que "la transferencia internacional de datos no debe afectar la protección de los interesados por lo que respecta al tratamiento de sus datos personales"[28].

Por eso, documentos internacionales como los citados exigen que para realizar transferencias internacionales de datos se asegure que existan "garantías comparables", un "nivel adecuado de protección", "protección equivalentes", "adecuado nivel de protección", y otras expresiones similares. Estos requerimientos son precisados

26 El "flujo de datos a través de las fronteras" o el "movimiento internacional de datos" son otras expresiones utilizadas para referirse a las transferencias internacionales de datos personales.

27 Garriga Domínguez, Ana. 2004. *Tratamiento de datos personales y derechos fundamentales*, Madrid: Dykinson, p. 177.

28 De Frutos, José Manuel. 2008. Globalización de la privacidad: hacia unos estándares comunes. Conferencia realizada en el VI Encuentro Iberoamericano de Protección de Datos, 27-30 de mayo del 2008, Cartagena, Colombia.

en las leyes de cada país, razón por la cual no se puede generalizar. En el caso de la regulación colombiana, por ejemplo, se prohíbe "la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos"[29]. La regulación colombiana es enfática en señalar con absoluta claridad que los estándares fijados para establecer si un país tiene dicho nivel "en ningún caso podrán ser inferiores"[30] a los que la Ley 1581 del 2012. Como se observa, para el caso colombiano no se puede enviar datos a un país que tenga un grado de protección inferior al previsto en la precitada norma.

La exportación y la importación de información personal no pueden convertirse en un escenario reductor del nivel de protección que se le confiere al titular del dato en el país desde donde se exportan datos personales, ni pueden ser un factor de riesgo para los responsables del tratamiento de datos, para quienes la información es un activo muy relevante, a tal punto que los datos personales son considerados la moneda de la economía digital. Dichas actividades no deben facilitar, permitir ni tolerar la vulneración de los derechos de las personas ni la disminución de las garantías con que cuentan en el país exportador.

• El principio de *accountability*

El término *accountability* (responsabilidad) proviene del mundo anglosajón[31] y a pesar de las diferentes acepciones que puedan darse de él, se ha entendido que

29 Cfr. República de Colombia, Ley 1581 del 2012, artículo 26.

30 Cfr. República de Colombia, Ley 1581 del 2012, artículo 26.

31 Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, p. 8.

en la arena de la protección de datos dicha expresión se refiere al modo como una organización debe cumplir en la práctica las regulaciones sobre la materia y a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente.

Garantizar la aplicación efectiva y práctica de lo que ordenan las normas sobre protección de datos es un reto permanente de cualquier organización. El principio de responsabilidad cobra cardinal importancia para lograr ese propósito. Dicho principio exige que los responsables y encargados del tratamiento de datos, implementen medidas apropiadas, efectivas y verificables que les permitan probar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, el Programa Integral de Gestión de Datos Personales (PIGDP) se constituye en un mecanismo operativo para realizar todo lo necesario con miras a garantizar el debido tratamiento de los datos personales.

El principio de responsabilidad demostrada puede ser igual de útil o de inútil que las leyes, si en la práctica, las organizaciones no hacen nada para cumplir uno u otro. Por eso, los resultados esperados de la aplicación de dicho principio dependerán del grado de compromiso y seriedad de la organización para materializar en el tratamiento de datos lo que ordenan las regulaciones e, incluso, ir más allá con medidas proactivas que generen valor agregado para garantizar un adecuado tratamiento de datos personales y proteger activos o intereses de la organización en cuanto a la explotación económica o el uso de los datos para los fines que los requiere.

Por eso, el reto de las organizaciones frente al principio de responsabilidad va mucho más allá de la expedición de documentos, porque exige que se demuestre el cumplimiento real y efectivo cuando realizan sus funciones.

No existe una fórmula única y estándar para implementar el principio de responsabilidad demostrada en las organizaciones, sino que este debe estar acompañado de

medidas ajustadas a la realidad específica de cada organización y teniendo en cuenta, entre otros, la disponibilidad de recursos, la naturaleza de los datos que trata en sus sistemas de información y los riesgos que implica para el titular y para los responsables el tratamiento de información personal.

El principio de responsabilidad demostrada —*accountability*— ha sido incorporado en los principales documentos sobre tratamiento de datos personales de las siguientes organizaciones: Red Iberoamericana de Protección de Datos (RIPD); la Unión Europea (UE); la Organización de Estados Americanos (OEA); la Organización para la Cooperación y el Desarrollo Económicos (OCDE); la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP); el Foro de Cooperación Económica Asia Pacífico (APEC) y la Organización de las Naciones Unidas (ONU).

De dichos documentos se observa lo siguiente: los primeros fueron emitidos en la década de los años ochenta y se referían a la responsabilidad pero sin necesidad de tener que demostrarla (era una especie de responsabilidad no demostrada). Algunos de ellos fueron modificados luego para ampliar su contenido e incluir la obligación de estar en capacidad de probar que los mecanismos son útiles, adecuados y eficientes.

La RIPD y la OCDE se destacan por describir aspectos más concretos sobre lo que se debe hacer para materializar la aplicación de dicho principio en la práctica cotidiana de las organizaciones. La RIPD especialmente sugiere mecanismos que el responsable debería adoptar para cumplir con el principio de responsabilidad. En la tabla n.º 2 (siguiente página) resumiremos algunos aspectos sobre esta cuestión.

Tabla n.º 2. Del principio de responsabilidad sobre tratamiento de datos personales incorporados en los principales documentos internacionales

Principio de responsabilidad demostrada (*accountability*)	**RIPD 2017**	**UE 2016**	**OEA 2015**	**OCDE 2013**	**CIAPDP 2009**	**APEC 2004**	**ONU 1990**
¿Está incluido expresamente en el documento?	✓	✓	✓	✓	✓	✓	X
¿Menciona expresamente que es aplicable a los sectores público y privado?	✓	✓		✓	✓		
¿Ordena implementar mecanismos para demostrar el cumplimiento de normas sobre TDP?	✓	✓	✓	✓	✓		
¿Enuncia herramientas para cumplir el principio de *accountability*?	✓	X	X	✓	X	X	
¿Ordena destinar recursos para la instrumentación de programas y políticas de TDP?	✓						
¿Propone implementar sistemas de administración de riesgos asociados al TDP?	✓			✓			
¿Ordena elaborar políticas y programas de TDP obligatorios y exigibles dentro de la organización del responsable?	✓			✓			
¿Incluye la necesidad de realizar programas de capacitación y actualización sobre TDP?	✓						
¿Sugiere revisar periódicamente las políticas y los programas de seguridad de datos personales para determinar las modificaciones que se requieran?	✓			✓			
¿Propone establecer un sistema de supervisión y vigilancia interna o externa, incluso auditorías, para comprobar el cumplimiento de las políticas sobre TDP?	✓						
Sugiere establecer procedimientos para recibir y responder dudas y quejas de los titulares?	✓			✓			
¿Ordena que se revisen y evalúen permanente-mente los mecanismos incorporados para cumplir con el principio de *accountability*?	✓						

Fuente: elaboración de Nelson Remolina Angarita©.
TDP: tratamiento de datos personales.

El principio de responsabilidad demostrada también se ha incluido en las regulaciones de algunos países latinoamericanos, como México y Colombia. En este último, por ejemplo, además de lo establecido en el Decreto 1377 del 2013, el Decreto 1413 del 2017[32] se refiere expresamente a la responsabilidad y los programas integrales de gestión de datos en los siguientes términos: Primero, obliga a los "operadores de servicios ciudadanos digitales" a adoptar "medidas apropiadas, efectivas y verificables que le[s] permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales"[33]. Luego, ordena a dichos operadores "crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales"[34]. Finalmente, establece que el PIGD deberá cumplir con "las instrucciones de la Superintendencia de Industria y Comercio, en particular, la guía para la implementación del principio de responsabilidad demostrada (*accountability*) de dicha entidad"[35].

• Necesidad de contar con una guía sobre *accountability* para las transferencias internacionales de datos

Varios motivos justifican que en las guías de *accountability* se desarrolle en detalle lo atinente a las transferencias internacionales de datos o la circulación transfronteriza en general.

32 Decreto 1413 del 25 de agosto del 2017, "Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el art. 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales".

33 Cfr. el artículo 2.2.17.6.3 del Decreto 1413 del 2017.

34 Cfr. ídem.

35 Cfr. ídem.

En primer lugar, como se ha mencionado, las transferencias internacionales junto con la protección de la intimidad fueron los dos principales motivos que generaron la regulación sobre tratamiento de datos personales. Por eso, ese tema no debe estar ausente de las guías de *accountability* ni, en caso que se incluya, ser tratado de manera superficial.

En segundo lugar, la responsabilidad digital de las empresas, la responsabilidad jurídica de los directivos, el comportamiento correcto y ético de las personas junto con el respeto de los derechos humanos son razones suficientes para incluir recomendaciones sobre transferencias internacionales en la guías de *accountability*.

Finalmente, las autoridades de protección de datos también han creado la necesidad de desarrollar este tema en las guías de *accountability*. En el caso de la República de Colombia, por ejemplo, mediante la Circular Externa 5 del 10 de agosto del 2017 de la Superintendencia de Industria y Comercio (SIC) —autoridad colombiana de protección de datos personales— ordenó lo siguiente en el parágrafo primero del numeral 3.2:

> Sin perjuicio de que las transferencias de datos personales se realicen a países que tienen un nivel adecuado de protección, los responsables del tratamiento, en virtud del principio de responsabilidad demostrada, debe ser capaces de demostrar que han implementado medidas apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia[36].

Como se observa, para transferir datos a otros países no es suficiente que el país de destino esté catalogado por la SIC como un país con nivel adecuado de protección,

36 Cfr. el numeral 3.2 de la Circular 5 del 2017 de la SIC.

sino que además es necesario que el responsable del tratamiento pueda demostrar que ha tomado medidas adecuadas, útiles y prácticas para lograr estos dos objetivos:

1. Garantizar el adecuado tratamiento de los datos personales que transfieren a otro país.
2. Conferir seguridad a "los registros al momento de efectuar dicha transferencia".

No obstante lo anterior, la guía de la SIC del 28 de mayo del 2015 sobre responsabilidad demostrada —*accountability*— no dice nada sobre las transferencias internacionales —*sólo menciona las transmisiones que son sustancialmente diferentes*—. En efecto, si bien los datos pueden salir de un país porque han sido transferidos, transmitidos o recolectados internacionalmente, en el caso de las transmisiones internacionales el responsable del tratamiento sigue siendo responsable del debido tratamiento de los datos que transmitió a un encargado ubicado o domiciliado en otro país.

Dado lo anterior, consideramos importante que existan medidas precisas, útiles y verificables que cualquier responsable del tratamiento debería adoptar antes de transferir los datos de los colombianos a otro país. Esto es necesario por las siguientes razones:

1. La transferencia internacional de datos vía responsabilidad demostrada es una cuestión novedosa sobre la cual hay mucho desconocimiento. No debe perderse de vista que la responsabilidad demostrada es una institución importada de otros sistemas jurídicos sobre la cual no ha habido mayor desarrollo práctico.

2. El principio de responsabilidad demostrada es una medida importada de otros sistemas jurídicos y poco conocida en el país a pesar de la existencia de la guía de la SIC. En la práctica, muchos responsables del tratamiento no saben qué hacer concretamente. Algunos tienen recursos para acudir a los servicios de empresas especializadas

en *accountability*, pero la mayoría carece de dinero para ese propósito. Así las cosas, la implementación real de la *accountability* dependerá, en muchos casos, de los recursos económicos de cada empresa, lo cual afectará la protección efectiva de los derechos de las personas cuyos datos son exportados por responsables del tratamiento que no tienen dinero.

3. Sugerencias sobre *accountability* y transferencias internacionales reducirían costos a las empresas —*porque por lo menos saben lo que deben hacer*— y establecerían unos mínimos para tratar de garantizar un cierto nivel de los derechos de las personas cuyos datos serán transferidos a otros países y proteger información estratégica de las organizaciones.

Visto lo anterior, a continuación presentamos nuestras sugerencias para implementar el principio de *accountability* en la circulación transfronteriza de datos.

II. Recomendaciones para implementar el principio de *accountability* en las transferencias internacionales de datos personales

- ### Verificar que está facultado para transferir o transmitir los datos personales a otro país

Antes de exportar los datos pregúntese lo siguiente: ¿Usted o su empresa está facultado(a) jurídicamente para poder exportar o enviar los datos personales a otro país? Es imprescindible que tenga plena certeza jurídica sobre este punto.

Si no está facultado, tenga presente que se expone a investigaciones administrativas o de naturaleza penal. Sobre este último aspecto, recuerde que la Ley 1273 del 2009 creó algunos tipos penales que sancionan, entre otros, ciertos aspectos relacionados con el tratamiento de datos personales como el acceso no autorizado a sistemas de información, la destrucción o manipulación de datos, la suplantación de sitios *web* para capturar datos personales y la violación de datos personales. Este último delito sanciona con prisión de cuatro a ocho años y multa de 100 a 1000 salarios mínimos legales mensuales a quien "*sin estar facultado* para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, *intercambie*, *envíe*, compre, intercepte, divulgue, modifique o emplee códigos personales, *datos personales* contenidos en ficheros, archivos, bases de datos o medios semejantes" (destacamos).

Como se observa, son diversas las conductas que generan responsabilidad penal en el tratamiento de datos personales. Esto hace que tanto los responsables como los encargados del tratamiento tengan que realizar una gestión muy cuidadosa y diligente para no incurrir en responsabilidad penal. Lo anterior es aún más grave si se tiene en cuenta que la pena señalada se aumenta de la mitad a las tres cuartas partes si la conducta la cometiere "[…] el responsable de la administración, manejo o control de dicha información". Además, dicha persona se expone a que se le imponga "hasta por tres años la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales".

- ## Determinar el mecanismo adecuado que utilizará para transferir o transmitir internacionalmente los datos personales

En línea con el punto anterior, debe determinarse cuál será el mecanismo que se utilizará para hacer circular la información en el ámbito transnacional. Hay que tener

presente que según el país, existen diversos caminos jurídicos para transferir datos personales, como los siguientes:

- transferencias basadas en la autorización del titular del dato;
- transferencias basadas en una decisión de adecuación;
- transferencias basadas en una declaración de conformidad;
- transferencias basadas en acuerdos *sui generis* (como el escudo de privacidad entre Europa y Estados Unidos [EU-US Privacy Shield]);
- transferencias mediante cláusulas contractuales;
- transferencias mediante normas corporativas vinculantes;
- transferencias mediante otro tipo de garantías adecuadas (códigos de conducta, mecanismos de certificación).

Sobre las menciones y los requisitos de cada una de las anteriores alternativas debe establecerse cuáles son permitidas por la regulación legal. En todo caso, para su aplicación puede tenerse como referencia lo previsto en documentos internacionales como los siguientes: 1. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril del 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), 2. Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017) de la Red Iberoamericana de Protección de Datos (RIPD).

- Establecer cómo se probarán las medidas de *accountability* para transferir los datos personales

En materia de responsabilidad demostrada o demostrable no basta hacer, sino probar lo que se hizo. Aunque existe libertad de utilizar diversos mecanismos probatorios, tenga presente que las normas de protección de datos imponen cargas probatorias que usted debe estar en capacidad de acreditar plenamente. Por eso, lo más práctico es suscribir contratos o documentos físicos o electrónicos que en un momento dado pueda presentar como prueba del cumplimiento de sus obligaciones.

- Tener en cuenta los objetivos que se deben cumplir según la regulación de su país para transferir datos internacionalmente

No es suficiente con estar legitimado para poder exportar los datos sino que es necesario verificar los propósitos que se deben cumplir según la regulación local de cada país.

- Asegurar el cumplimiento de las finalidades que se deben alcanzar con las medidas de *accountability*

Debe recordarse que las medidas de *accountability*, por lo menos, deben ser adecuadas y pertinentes para garantizar los siguientes objetivos establecidos en la Circular 5 del 2017 de la SIC:

1. Garantizar el adecuado tratamiento de los datos personales que transfieren a otro país.
2. Conferir seguridad a "los registros al momento de efectuar dicha transferencia".

El adecuado tratamiento de los datos personales supone, por lo menos, que en el país de destino de la exportación se respeten los derechos del titular del dato y que el tratamiento de datos en ese país garantice el cumplimiento de los principios de tratamiento de datos que exige la regulación del país desde donde se exporta la mencionada información.

- ## Crear estrategias para proteger los intereses de su organización

Evalúe los riesgos concretos que afrontará su organización por el mero hecho de transferir los datos personales a otros países y articule mecanismos para mitigarlos con herramientas contractuales, tecnológicas o de otra naturaleza.

- ## Adoptar medidas para no defraudar la confianza de sus clientes o de los titulares de los datos

El principio de *accountability* ha generado muchas expectativas y promesas. No obstante, puede ser un fracaso si no se hace nada para implementarlo en la práctica.

Si una empresa vive de sus clientes, hay que velar por la protección de los derechos de ellos y no dar motivos para perder su confianza. Si su organización es una entidad pública, recuerde que es deber constitucional proteger, entre otros, los derechos de las personas.

• Prever las transferencias ulteriores de datos personales

Hay que establecer reglas para el reenvío de los datos del país de destino inicial de la exportación de los datos a otros países. Tenga presente que si se deja esto sin control, al final del día los datos pueden terminar en países o empresas que en el práctica son paraísos informáticos.

• Incrustar la privacidad desde el diseño y por defecto en las transferencias internacionales de datos personales

La privacidad desde el diseño y por defecto tradicionalmente se ha considerado otra medida proactiva, pero en algunos casos se le ha catalogado como un principio en el tratamiento de datos. A continuación nos referiremos a dicha medida dados los objetivos que se quiere alcanzar y teniendo en cuenta que de ella se pueden aplicar analógicamente muchas cuestiones a las transferencias y transmisiones de datos personales.

La privacidad por diseño (PbD, por sus iniciales en inglés) fue definida y desarrollada desde la década de los años noventa por Ann Cavoukian, quien considera que "el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización"[37]. Para el efecto, ella propone los siguientes principios que pueden ser aplicados o adaptados a las transferencias internacionales y que son consistentes con el principio de *accountability*:

37 Cfr. Cavoukian, Ann (2011). *Privacy by Design. Los 7 Principios Fundamentales.* Disponible en https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf.

– *Proactivo, no reactivo; preventivo no correctivo*. Según este principio, se debe adoptar medidas proactivas y no reactivas para proteger los datos personales. Según Cavoukian, la PbD "no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron; su finalidad es prevenir que ocurran. En resumen, privacidad por diseño llega antes del suceso, no después"[38].

En el caso de las transferencias internacionales, se deben adoptar medidas para prevenir cualquier incidente respecto de ellas y no esperar a que ocurra un problema para adoptar medidas reparadoras.

– *Privacidad como la configuración predeterminada*. Este principio parte de que "Lo predeterminado es lo que manda"[39], por eso se quiere que la protección de datos haga parte de lo predeterminado. Por lo tanto, se debe asegurar que "los datos personales estén protegidos automáticamente en cualquier sistema de IT dado o en cualquier práctica de negocios"[40].

Teniendo en cuenta lo anterior, las estrategias de debido tratamiento de datos deben hacer parte de los aspectos cruciales que han de involucrarse desde un principio en los procesos de circulación internacional de datos personales.

– *Privacidad incrustada en el diseño*. En línea con lo anterior, la privacidad y el debido tratamiento de datos deben hacer parte del diseño y la arquitectura del *software*, los dispositivos tecnológicos y la operatividad de las empresas y las organizaciones. Con esto se quiere que "la privacidad se convierte en un componente esencial de la

38 Cfr. ídem.

39 Cfr. ídem.

40 Cfr. ídem.

funcionalidad central que está siendo entregada. La privacidad es parte integral del sistema, sin disminuir su funcionalidad"[41].

– *Funcionalidad total: "Todos ganan", no "Si alguien gana, otro pierde"*. Con este principio se quiere recalcar que los negocios o las actividades de las organizaciones no son incompatibles y no deben plantearse de unas cosas versus otras, sino buscar un punto de equilibrio. Según Cavoukian, "Privacidad por diseño busca acomodar todos los intereses y objetivos legítimos de una forma 'ganar-ganar', no a través de un método anticuado de 'si alguien gana, otro pierde', donde se realizan concesiones innecesarias"[42].

– *Seguridad extremo-a-extremo – Protección de ciclo de vida completo*. Si la seguridad se incorpora en los procesos desde el inicio, ello contribuye a garantizarla durante todo el ciclo de tratamiento de los datos personales.

Tenga presente que la seguridad de la información no es solo algo que beneficia al titular del datos sino que es muy importante para el responsable de los datos que considere que la información es un bien valioso para su organización y buena reputación.

– *Visibilidad y transparencia – Mantenerlo abierto*. Se quiere que las promesas que se hagan a las personas sobre la privacidad y el tratamiento de datos se cumplan en la práctica y que ellas se puedan verificar.

– *Respeto por la privacidad de los usuarios – Mantener un enfoque centrado en el usuario*. "Por encima de todo, la privacidad por diseño requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas, ofreciendo medidas tales como predefinidos de privacidad robustos, notificación apropiada, y

41 Cfr. ídem.

42 Cfr. ídem.

facultando opciones amigables para el usuario. Hay que mantener al usuario en el centro de las prioridades"[43].

En la regulación colombiana, el Decreto 1413 del 2017[44] no solo define la privacidad por diseño como "la protección de la información que exige la incorporación en las especificaciones de diseño de tecnologías, procesos, prácticas de negocio e infraestructuras físicas que aseguren la protección de la privacidad de la información"[45], sino que la considera un principio cuyo alcance es el siguiente:

> […] desde antes [de] que se recolecte información y durante todo el ciclo de vida de la misma [*sic*], se deben adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental) para evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como fallas de seguridad o indebidos tratamientos de datos personales. La privacidad y la seguridad deben hacer parte del diseño, [la] arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan[46].

El decreto obliga a los operadores a aplicar las buenas prácticas y principios desarrollados internacionalmente sobre los "privacy by design (PbD)" y "privacy impact assessment (PIA)", señalando que

43 Cfr. ídem.

44 Colombia. Decreto 1413 del 25 de agosto del 2017, "Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales".

45 Cfr. el numeral 17 del artículo 2.2.17.1.3 del Decreto 1413 del 2017 (Colombia).

46 Cfr. el numeral 6 del artículo 2.2.17.1.5 del Decreto 1413 del 2017 (Colombia).

> la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, [el] uso, almacenamiento, [la] divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador[47].

Para lograr lo anterior, los operadores deben tener presentes las siguientes pautas:

1. Realizar y actualizar las evaluaciones del impacto de tratamiento de los datos personales y el Programa Integral de Gestión de Datos Personales ante cambios que generen riesgos de privacidad.
2. Incorporar prácticas y procesos de desarrollo necesarios destinados a salvaguardar la información personal de los individuos a lo largo del ciclo de vida de un sistema, programa o servicio.
3. Mantener las prácticas y procesos de gestión adecuados durante el ciclo de vida de los datos que son diseñados para asegurar que sistemas de información cumplen con los requisitos, políticas y preferencias de privacidad de los ciudadanos.
4. Uso de los máximos medios posibles y necesarios para garantizar la seguridad, confidencialidad e integridad de información personal durante el ciclo de vida de los datos, desde su recolección original, a través de su uso, almacenamiento, difusión y segura destrucción al final del ciclo de vida.

47 Cfr. el artículo 2.2.17.6.5 del Decreto 1413 del 2017 (Colombia).

5. Asegurar la infraestructura, los sistemas TI y prácticas de negocios que interactúan o implican el uso de cualquier información o dato personal siendo sujeta a verificación independiente por parte de todas las partes interesadas, incluyendo clientes, usuarios y organizaciones afiliadas[48].

• Replicar medidas proactivas del tratamiento de datos personales a las transferencias internacionales de dicha información

Internacionalmente se ha recomendado la implementación de medidas proactivas de protección de datos con miras a mejorar el cumplimiento de las normas sobre protección de datos, así como consolidar y fortalecer el debido tratamiento de datos personales en las organizaciones. Dentro de dichas herramientas se encuentran, entre otras, las siguientes:

– *Designar un delegado de protección de datos*. Esta persona podría ser, entre otras, la encargada de verificar que en la organización se cumplan todos los requerimientos legales y las exigencias de la autoridad de protección de datos para transferir datos a otros países. Además, sería la que se responsabilizaría de realizar planes de monitoreo y evaluación respecto del tratamiento de los datos exportados.

– *Evaluar impacto de privacidad o de protección de datos*. Según el caso, estos estudios son útiles en proyectos de gran impacto o de alto riesgo que involucren, por ejemplo, el tratamiento de datos personales sensibles o de menores de edad.

48 Cfr. el artículo 2.2.17.6.5 del Decreto 1413 del 2017 (Colombia).

– *Capacitar y entrenar de manera especializada*. Realizar periódicamente actividades de educación y entrenamientos específicos a las personas a cargo de enviar datos personales a otros países con el fin de verificar si cuentan con la preparación suficiente y especializada para realizar transferencias o transmisiones internacionales de datos personales.

– *Implementar planes de monitoreo y evaluación*. Según el caso, resulta pertinente que el responsable (exportador de los datos) pueda realizar monitoreo o auditorías al responsable o encargado ubicado en el país destinatario de los datos para que verifique si éste está cumplimiento adecuadamente con sus obligaciones respecto de, entre otras, seguridad, uso debido de los datos, confidencialidad.

– *Adherir acuerdos de autorregulación*.

– *Implementar planes de contingencia*. Hay que fijar desde el principio las pautas o acciones que seguirá frente a situaciones graves o inesperadas respecto de los datos enviados a otro país. Por ejemplo: ¿qué haría en caso de que se presente un ataque informático que comprometa la seguridad y confidencialidad de los datos transferidos o transmitidos a otro país?

• Articular las herramientas de *accountability* en un contrato ajustado a las particularidades de cada transferencia

Los contratos representan una alternativa jurídica para demostrar la implementación de medidas de *accountability* en las transferencias internacionales de datos. Aunque existen modelos de contratos[49] en esta materia, es crucial que el contrato

49 La Comisión de las Comunidades Europeas, por ejemplo, adoptó las decisiones 2001/497/CE, 2004/915/CE y 2010/78/CE mediante las que avala ciertas cláusulas contractuales tipo para la transferencia de datos

sea consistente con las peculiaridades y necesidades de cada organización. Así mismo, es relevante que el exportador de los datos trate de establecer si el receptor de los datos en otro país es una empresa u organización seria (no un paraíso informático) que cumplirá las obligaciones contractuales.

Para la redacción del contrato, tenga presente varios aspectos:

- La naturaleza jurídica de los datos que se exportarán a otro país. Según sea aquella (sensible, de menores de edad, privada, semiprivada, pública), pacte medidas especiales de protección. Recuerde, por ejemplo, que para el tratamiento de datos sensibles se exige una responsabilidad reforzada, es decir, mayores medidas de seguridad, mayores restricciones de acceso, uso y circulación.
- Las medidas de seguridad que debe cumplir el destinatario (importador) de los datos exportados a otro país.
- La cantidad de datos que se exportarán.
- ¿Cuáles son los derechos que el destinatario de la información o importador debe garantizar al titular del dato?
- ¿Cuáles son los principios del tratamiento de datos personales que el importador o destinatario de los datos debe observar o garantizar?
- ¿Quiénes podrán tener acceso a la información exportada?

---

personales. Las decisiones 2001/497/CE y 2004/915/CE sugieren modelos de contratos cuando la administración de los datos personales pasa de un operador a otro que se encuentra en un país diferente, mientras que la Decisión 2010/78/CE comprende un esquema de contrato para aquellos casos en que la administración de la información está bajo responsabilidad de un operador que acude a un tercero ubicado en otro país para que se encargue del tratamiento de ellos.

- Los mecanismos para que el titular del dato pueda ejercer sus derechos de manera sencilla y expedita ante el destinatario de los datos exportados.
- Las finalidades para las cuales se transfiere los datos. Es muy importante dejar claro qué puede y qué no puede hacer el destinatario de los datos transferidos.
- ¿Cuál será el límite de tiempo durante el cual el destinatario de los datos transferidos podrá tratarlos?
- La ley de protección de datos que regirá el contrato. Será la ley del país del exportador de los datos o la del importador de estos. Si se quiere garantizar el principio de "continuidad de protección de datos" a que nos referimos en este documento, lo recomendable es que el contrato se rija por la ley de protección de datos del país desde donde se exportarán.
- La posibilidad o no de realizar transferencias ulteriores a otros países. Deje claro si los datos inicialmente transferidos a un país A pueden ser transferidos luego desde ese país A a otro país B. En caso positivo, establezca las condiciones que se deben observar para dicho efecto.
- ¿Qué hacer para recuperar los datos transferidos y garantizar los derechos de los titulares de ellos cuando el destinatario de la exportación incumpla el contrato?
- ¿Quién o quiénes responderán ante la autoridad de protección de datos o los titulares de los datos por un eventual indebido tratamiento de la información exportada y por los daños y perjuicios causados?
- Cuál será la responsabilidad (conjunta o solidaria) del exportador y del importador de los datos frente al titular de estos por las eventuales vulneraciones de sus derechos o los daños y perjuicios causados?
- ¿Qué se hará con los datos una vez termine el contrato?

- Articular estas recomendaciones con la guía de *accountability* de la autoridad de protección de datos

Finalmente, es importante recalcar que todas las sugerencias anteriores sólo están enfocadas para implementar el principio de *accountability* en la circulación transfronteriza de datos personales, ya sea a través de transferencias o mediante transmisiones internacionales de datos. Como tal, esta guía es de carácter especial y complementario a las guías generales que sobre la materia han expedido las autoridades de protección de datos.

En el caso de Colombia, por ejemplo, la SIC expidió el 28 de mayo del 2015 la *Guía para implementación del principio de responsabilidad demostrada (accountability)*, que replica, en buena medida, la guía de canadiense de *accountability* titulada *Getting Accountability Right with a Privacy Management Program*[50], expedida en el 2012 por la Oficina del Comisionado de Privacidad de Canadá. Otra guía de referencia puede ser la de Hong Kong, denominada *Implementing and Demonstrating Accountability*[51], expedida el 11 de febrero del 2014 por la Oficina del Comisionado de Privacidad para Datos Personales de Hong Kong.

50 El texto de la guía puede consultarse en https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf.

51 El texto de la guía puede consultarse en https://www.pcpd.org.hk/privacyconference2014/files/9_booklet_guide.pdf.

Glosario

Las siguientes definiciones en algunos casos replican y en otros tienen en cuenta lo dispuesto por la legislación de la República de Colombia. Es factible que ellas coincidan o no con lo señalado en las regulaciones de otros países:

Autorización: "Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales"[52].

Dato personal: "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"[53].

Encargado del tratamiento: "Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros realice el tratamiento de datos personales por cuenta del responsable del tratamiento"[54].

Exportador: Persona u organización que envía datos personales de un país a otro u otros países.

Internet de las empresas (*Internet of corporations*): Normas que los empresarios han creado para realizar negocios o prestar servicios en la internet. Se trata de las pautas que los empresarios consideran sensatas bajo su modelo de negocios

52 Cfr. el literal *a* del artículo 3.º de la Ley 1581 del 2012.

53 Cfr. el literal *c* ibídem.

54 Cfr. el literal *d* ibídem.

para ganar utilidades en la economía digital. Ejemplo de estas normas son las notales legales o los términos y condiciones en las páginas *web* o las app y los demás servicios en la internet.

Importador: Persona u organización destinataria o receptora de la información exportada.

Paraísos informáticos (*data havens*): País o empresa en donde la protección de los derechos de los titulares de los datos es débil o inexistente.

Recolección internacional de datos personales: Actividad mediante la cual una empresa u organización domiciliada en un país recoge o recauda datos de personas ubicadas en otro país. Los datos son recolectados directamente del titular del dato y con el uso de tecnologías o herramientas como páginas *web*, app o *cookies*.

Responsable del tratamiento: "Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros decida sobre la base de datos o el tratamiento de los datos"[55].

Titular del dato: "Persona natural cuyos datos personales sean objeto de tratamiento"[56].

Transferencia internacional de datos: "La transferencia de datos tiene lugar cuando el responsable o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país"[57].

55 Cfr. el literal *e* ibídem.

56 Cfr. el literal *f* ibídem.

57 Cfr. el numeral 4 del artículo 2.2.2.25.1.3 del Decreto 1074 del 2015 (Decreto 1377 del 2013, artículo 3.º).

Transmisión internacional de datos: "Tratamiento de datos personales que implica la comunicación de los mismos [*sic*] fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable"[58].

Tratamiento: "Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"[59].

58 Cfr. el numeral 5 ibídem.

59 Cfr. el literal *g* del artículo 3.º de la Ley 1581 del 2012.

Bibliografía

Accenture. 2016. Guarding and growing personal data value Organizations that demonstrate responsibility in the way they handle personal data today will lead the digital economy of tomorrow. Enero. En https://www.accenture.com/us-en/insight-guarding-growing-personal-data-value.aspx.

Cano Martínez, Jeimy. 2016. ¿Eres una empresa digitalmente responsable? Enero 20. En https://www.linkedin.com/pulse/eres-una-empresa-digitalmente-responsable-jeimy-cano-ph-d-cfe.

Cano Martínez, Jeimy. 2014. Presiones emergentes sobre la privacidad de la información, en http://insecurityit.blogspot.com.co/2014/05/presiones-emergentes-sobre-la.html.

Montezuna, Alberto. 2017. Colombian draft regulation introduces accountability principle to data transfers, en https://iapp.org/news/a/colombian-draft-regulation-introduces-accountability-principle-to-data-transfers.

Palazzi, Pablo. 2003. Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado. En *Derecho de internet & telecomunicaciones*, editado por el GECTI. Bogotá: Legis.

Parmar, R., Mackenzie, I., Cohn, D. y Gann, D. (2014) The new patterns of innovation. *Harvard Business Review*. January-February. Disponible en https://hbr.org/2014/01/the-new-patterns-of-innovation.

Puccinelli, Oscar. 1999. *El* habeas data *en Indoiberoamérica*, primera edición, Bogotá: Temis.

Remolina Angarita, Nelson. (2016) "Internet de las empresas" ["Internet of Corporations" -IoC-]: una explicación de lo que pasa en internet y del futuro de la protección de los derechos humanos en el ciberespacio (parte 1). Universidad de los Andes. Publicado en https://habeasdatacolombia.uniandes.edu.co/?p=2222.

Remolina Angarita, Nelson. 2015. Recolección internacional de datos: un reto del mundo postinternet. BOE – *Boletín Oficial del Estado*. Madrid, abril del 2015. ISBN 978-84-340-2196-9.

Remolina Angarita, Nelson. 2013. *Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012*. Bogotá, Legis, 2013. ISBN 978-958-767-086-8.

Remolina Angarita, Nelson. 2012. Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales* –RIPDP–. Red Académica Internacional de Protección de Datos Personales (1):1-13.

Remolina Angarita, Nelson. 2010. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 *International Law, Revista Colombiana de Derecho Internacional*, 489-524 (2010).

Remolina Angarita, Nelson. 2010. Cláusulas contractuales y transferencia internacional de datos personales, en *Obligaciones y contratos en el derecho contemporáneo*, 357-419, Jorge Oviedo-Albán (ed.), Bogotá, Biblioteca Jurídica Diké y Universidad de La Sabana.

Equipo de trabajo

Para la redacción de esta guía se conformó un equipo de trabajo integrado por:

Nelson Remolina Angarita

Doctor (*Ph. D.*) *Summa Cum Laude* en Ciencias Jurídicas de la Pontificia Universidad Javeriana (Bogotá). Master of Laws, The London School of Economics and Political Sciences (Londres). Especialista en Derecho Comercial y abogado egresado de la Universidad de los Andes. Director del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Universidad de los Andes y del Observatorio Ciro Angarita Barón sobre protección de datos personales. Ganador del Premio Protección de Datos Personales de Investigación 2014, conferido por la Agencia Española de Protección de Datos (AEPD) sobre trabajos originales e inéditos que traten acerca del derecho a la protección de datos en países iberoamericanos. Profesor asociado y director de la Especialización en Derecho Comercial de la Universidad de los Andes.

Autor de varios libros y artículos sobre tratamiento de datos personales. Su tesis doctoral se centró en el estudio de las transferencias y la recolección internacional de datos personales.

Luisa Fernanda Álvarez Zuluaga

Abogada egresada de la Universidad de los Andes. Cuenta con experiencia en investigación internacional sobre el principio de *accountability*, los programas integrales de gestión de datos y las guías de *accountability*.

Universidad de los Andes
Colombia

GECTI

Observatorio Ciro Angarita Barón
sobre la protección de datos personales

https://gecti.uniandes.edu.co
https://habeasdatacolombia.uniandes.edu.co