Fecha de recepción: 21 de mayo de 2012 / Fecha de aprobación: 4 de junio de 2012

Revista de Derecho Comunicaciones y Nuevas Tecnologías

Normas corporativas vinculantes y transferencias internacionales de datos personales: elementos para su reglamentación

Luis Alberto Montezuma Chávez

Universidad de los Andes
Facultad de Derecho
Revista de Derecho, comunicaciones y Nuevas Tecnologías
N.º 8, Diciembre de 2012. ISSN 1909-7786

Normas corporativas vinculantes y transferencias internacionales de datos personales: elementos para su reglamentación

Luis Alberto Montezuma Chávez*

Resumen

Este escrito es resultado de la investigación realizada como estudiante de la Maestría en Derecho Privado de la Universidad de los Andes. En este artículo se establecen los requisitos y condiciones que deben reunir las Normas Corporativas Vinculantes (NCV), para ser un instrumento que permita la transferencia internacional de datos a terceros países. De igual forma, propone los elementos esenciales que el Gobierno Nacional debería considerar y abordar en la futura reglamentación de las NCV, con miras a que las mismas contribuyan de manera efectiva a garantizar un debido tratamiento de los datos personales cuando sean objeto de transferencia internacional.

Palabras clave: nivel adecuado de protección de datos, normas corporativas vinculantes, medidas adecuadas y eficaces, grupo corporativo,

Abstract

This document is a result of an investigation made as a student of the master's in Private Law of the Universidad de los Andes. This article sets out the requirements and conditions to be met by the Binding Corporate Rules (BCR´s) to be an instrument for the international transfer of data to third countries. The same shall propose the essential elements that the Government should consider and address in the future regulation of BCR´s with a view to effectively help them to ensure a proper treatment of personal data which are subject to international transfer.

Keywords: Adequate data level protection; Binding Corporate Rules; Adequate and effective measures; Corporate Group; Data protection responsible; Treatment attendant; Third party beneficiary; Self-regulation; programs and stamp certifications; responsible authorities of data protection.

* Abogado de la Universidad Libre. Especialista en Legislación Financiera de la Universidad de los Andes. Candidato a Máster en Derecho Privado en la Universidad de los Andes. Director Jurídico de Acciones Constitucionales S.A.S. Correo electrónico: luismontezumachavez@gmail.com

responsable del tratamiento de datos, encargado del tratamiento, tercero beneficiario, autorregulación, programas o sellos de certificación, autoridades responsables de la protección de datos.

Sumario

Introducción

Antonio Troncoso Reigada (2010, p. 252) en su libro *La protección de datos personales. En búsqueda del equilibrio,* señala que: "La defensa de la privacidad se muestra (...) como una oportunidad de negocio y de ventaja competitiva para las empresas". Los grupos corporativos necesitan que la información de sus clientes o empleados fluya a nivel global sin trabas regulatorias para el desarrollo de su gestión. Por ejemplo, una empresa ubicada en Colombia puede trasladar los datos de sus empleados a una sucursal localizada en Turquía. Las empresas requieren de regímenes normativos que se ajusten a la dinámica propia del mercado, y que coadyuven a su desarrollo.

Por otra parte, tenemos que un objetivo de la política normativa de los Estados es evitar la transferencia de datos personales a destinos donde se carece de legislación en la materia, es insuficiente o donde no existen los mecanismos eficaces que garanticen su protección, conocidos como "paraísos de datos". Para Mauricio Domingo Donovan (2012, p. 3) "el uso indebido de datos personales por parte de un particular puede tener consecuencias gravísimas para una persona; desde recibir montones de publicidad no deseada o llamadas publicitando algún producto o servicio en la privacidad de nuestro hogar, o incluso en nuestro celular, hasta el robo de identidad". Vemos la importancia en que los países protegan la vida privada de sus ciudadanos en el tratamiento de sus datos personales y al margen, si estos guardan relación con la vida privada, se asegure un debido tratamiento de los mismos en cada país y, especialmente, cuando estos son transferidos de un país a otro.

Los europeos han sido precursores en materia de regulación de información de carácter personal. En efecto, en la Unión Europea solo se autoriza la libre circulación de datos de sus ciudadanos a terceros países que ofrezcan un nivel "adecuado" o "equiparable" de protección[1]. El tercer país, bien sea actuando como responsable o encargado del tratamiento, debe ofrecerle al sujeto iguales o superiores derechos y garantías en la protección de su información al régimen europeo. No obstante, para la UE si el país de destino no proporciona ese nivel "comparable", el exportador de datos puede aportar las garantías adecuadas, a saber, "cláusulas contractuales" o "normas corporativas vinculantes", para legalizar la operación.

Las Normas Corporativas Vinculantes (NVC) son un sistema de "autorregulación", creado para facilitar la transferencia de datos personales a nivel multinacional, materializado a través de un conjunto de derechos y garantías para las personas; y deberes, obligaciones y responsabi-

1 Cfr. (i) Suiza (Decisión de la Comisión 200/518/CE, de 26 de julio de 2000); (ii) Hungría (Decisión de la Comisión 200/519/CE, de 26 de julio de 2000); (iii) Las entidades estadounidenses adheridas a los principios de "Puerto Seguro" (Decisión 2000/520/CE de la Comisión de 26 de julio de 2000; (iv) Canadá (Decisión 2002/2/CE de la Comisión de 20 de diciembre de 2001); (v) Argentina (Decisión 2003/490/CE, de la Comisión de 30 de junio de 2003; (vi) Bailía de Guernsey (Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003); (vii) Islas del Man (Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004); (viii) Isla Jersey (Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008); (ix) Islas Feroe (Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010); (x) Andorra (Decisión 2010/146/UE de la Comisión de 5 de marzo de 2010); e, (xi) Israel (Decisión de la Comisión de 31 de enero de 2011 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo). Consultar la página de la Agencia Española de Protección de Datos. En https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides idphp.php.

lidades para el grupo corporativo, encaminado al cumplimiento efectivo de los principios relativos a la protección de la información de carácter personal.

Colombia adoptó esta figura en el artículo 28 del Proyecto de Ley del Senado Número 184 y 046 de la Cámara del 2010[2] (Hoy artículo 27 de la Ley 1581 de 2012), que cita: "El Gobierno Nacional expedirá la reglamentación correspondiente sobre Normas Corporativas Vinculantes para: (i) la certificación de buenas prácticas en protección de datos personales; y, (ii) su transferencia a terceros países", artículo que fue encontrado ajustado a la norma constitucional, y declarado exequible por parte de la Corte Constitucional mediante Sentencia C-748 de 2011, M.P. Jorge Ignacio Pretelt Chaljub[3].

Los objetivos del presente artículo son: en primer lugar, establecer los requisitos y condiciones que deben reunir las NCV, para ser un instrumento que permita la transferencia internacional de datos a terceros países; y, en segundo lugar, y con ocasión del ejercicio anterior, dejar planteados los elementos esenciales que el Gobierno Nacional debería considerar y abordar en la futura reglamentación de las NCV con miras a que las mismas contribuyan de manera efectiva a garantizar un debido tratamiento[4] de los datos personales cuando sean objeto de transferencia internacional.

Para lograr lo anterior, se explica, en primer término, en qué consisten las NCV. Partiendo de este punto, se definirá de manera general qué es: (i) "transferencia internacional de datos"; (ii) "nivel adecuado de protección de datos"; (iii) "garantías adecuadas"; y, (iv) "autorregulación".

En segundo término, es pertinente descomponer y entender la estructura de las NCV, diseñada desde la perspectiva de la regulación Europea (es claro que Colombia ha incorporado normativamente la experiencia de la UE en la materia)[5]. Este aspecto sirve para evaluar si las empresas están efectivamente obligadas por las normas corporativas, garantizando la protección de los derechos de los involucrados en el tratamiento de los datos. Es importante tener

2 En la exposición de motivos del Proyecto de Ley del Senado Número 184 y 046 de la Cámara del 2010 (hoy Ley 1581 de 2012), se indicó que: "la transferencia de datos a terceros países constituye uno de los principales elementos para la protección efectiva de los datos personales ya que si bien se exige una protección efectiva en el territorio nacional también se protege que los datos de ciudadanos nacionales o extranjeros que se hayan tratado en el país no puedan ser enviados a países que no cumplen con los requisitos mínimos de protección tal y como lo contempla la legislación nacional" (Congreso de la República, 2010).

3 La Corte Constitucional indicó que: "la delegación que hace la norma para que sea el Gobierno Nacional el que reglamente los contenidos mínimos que deben contener estas normas corporativas se ajusta a la Constitución, pues en desarrollo de los principios que rigen la administración de los datos personales, estos códigos de conducta para las buenas prácticas en esta materia, se convierten en un instrumento adicional para la efectiva garantía del derecho al hábeas data".

4 El Proyecto de Ley del Senado Número 184 y 046 de la Cámara del 2010 (hoy Ley 1581 de 2012), define como tratamiento "cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión". La Corte Constitucional, en la sentencia de constitucionalidad del proyecto de Ley, señaló que: "cuando el proyecto se refiere al tratamiento hace alusión a cualquier operación que se pretenda hacer con el dato personal, con o sin ayuda de la informática, pues a diferencia de algunas legislaciones, la definición que aquí se analiza no se circunscribe únicamente a procedimientos automatizados".

5 En la exposición de motivos del Proyecto de Ley del Senado Número 184 y 046 de la Cámara del 2010 (hoy Ley 1581 de 2012), se señaló que: "este proyecto incorpora en su articulado las mejores prácticas internacionales en materia de protección de datos contempladas en [el] Convenio 108 de 1981 del Consejo de Europa, la Directiva Europea 95/46 de 1995, la Resolución 45/95 de 1990 de la ONU y la Resolución de Madrid de 2009, con el objetivo de lograr con esta ley la acreditación de Colombia por parte de la Unión Europea como un país seguro en protección de datos y así poder acceder al mercado europeo sin restricciones atrayendo inversión extranjera y generando nuevos empleos" (Congreso de la República, 2010).

presente que el objetivo de un sistema de "autorregulación" es que su política interna efectivamente se cumpla en la práctica por la organización empresarial.

Finalmente, en el último capítulo se explora el significado de los "modelos de certificación", diseñados para acreditar que las NCV se adecuan a la regulación en materia de privacidad y protección de datos personales. Al respecto, conviene tener en cuenta los "sellos de certificación" incorporados en la legislación mexicana.

I. APROXIMACIÓN GENERAL A UN SISTEMA DE AUTORREGULACIÓN: TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Para el profesor Francisco J. Cruz Fuenzalida (2010, pp. 6-7)[6], las NCV "son reglas de conducta vinculantes", que fijan estándares para las transferencias internacionales dentro de grupos multinacionales de empresas, que gozan de mayor flexibilidad para la exportación e importación de datos; definición que será ampliada en el capítulo II del presente escrito, lo que nos lleva a tener en cuenta dos aspectos jurídicos a explicar en este documento. El primero va relacionado con la definición de "flujo transfronterizo de datos personales". Y el segundo, respecto de la implementación de sistemas de "autoevaluación" en la circulación internacional de información de carácter personal.

A. Transferencia internacional de datos personales

Para Rosa Barceló y María Verónica Pérez Asinare (2008, pp. 162-163), "una problemática particular que se plantea respecto de las empresas multinacionales es que cuentan con ficheros de datos personales que son compartidos entre todas las filiales del grupo, a menudo en los cinco continentes". Asimismo, Nelson Remolina (2010, p. 376), citando a María José Blanco, indica que: "en el plano empresarial, las multinacionales requieren circular información entre las diferentes sucursales o establecimientos que poseen a lo largo del planeta. Otras empresas requieren de la misma para brindar atención telefónica a los clientes a través de *call center* internacionales, realizar acciones de marketing telefónico, administrar, proveer y dar soporte técnico a las bases de datos de clientes y proveedores". Como se verá en la siguiente gráfica, el almacenamiento y procesamiento de los datos de los interesados puede terminar administrado en una filial(es) ubicada(s) en uno de los cinco continentes, diferente al país donde se recolectó la información.

6 Las medidas tendientes al resguardo de los datos ayudan a uniformar las políticas de Privacy by Design(10) (PbD), denominación que apunta a la protección de la información desde el origen de las operaciones y no sólo cuando éstas puedan constituir un riesgo, promoviendo también la autorregulación. Cruz, F.J. (2010, pp. 6-7).

Figura 1. Exportación e importación[7] de la información de los titulares de un país a otro sin un control en las fronteras nacionales.

Fuente: aerocolombia.com, 2011.

El "movimiento internacional de datos" supone el traslado de la información personal, que se encuentra previamente recolectada en ficheros o bases de datos, a empresas ubicadas fuera del territorio donde se originó la misma; así, por ejemplo, una sociedad ubicada en la China puede transmitir los datos de sus empleados a otra sociedad ubicada en el Brasil. En ese sentido, María Arias Pou (2006, p, 515), en el libro *Manual Práctico de Comercio Electrónico*, indica que: "hay transferencia internacional de datos cuando comunicamos o cedemos datos personales a un responsable del fichero extranjero y cuando encargamos a una persona física o jurídica extranjera la prestación de un servicio para la que sea necesaria la transmisión de datos"[8]. La libre circulación internacional de datos de carácter personal ya ha sido aceptada por diversos sistemas normativos, siempre y cuando, el país receptor de la información tenga un nivel "adecuado" de protección, como veremos a continuación.

En la Unión Europea se ha establecido un conjunto de reglas para el flujo transfronterizo de datos personales, con el Convenio 108 del 28 de enero de 1981, entre otros[9]. En la parte in-

7 Estas expresiones se han contextualizado en la regulación Española sobre protección de datos. En efecto, el literal j, del artículo 5 del Real Reglamento (RDLOPD), que desarrolla la Ley Orgánica 15 del 13 de diciembre de 1999, Protección de Datos de Carácter Personal (LOPDCP), define al exportador de datos como aquella "persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero". El literal ñ, del citado artículo, define al importador como aquella "persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero".

Véase también que la norma primera, sección primera, de la Instrucción 1/2000, de la Agencia Española de Protección de Datos (AEPD), relativa a las normas por las que se rigen los movimientos internacionales de datos, define la transferencia internacional de datos como "toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero". Consúltese la primera parte de las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales adoptadas por la Organización para la Cooperación y el Desarrollo Económico (OCDE), 23 de noviembre de1980, que define la "circulación transfronteriza de datos personales", como "movimientos de datos personales a través de fronteras nacionales".

Sobre la definición del "movimiento internacional de datos, léase a Cecilia Álvarez Rigaudias, "Las transferencias internacionales de datos personales y el nivel equiparable o adecuado de protección de datos". Actualidad Jurídica Uría Menéndez/12-2005. Recuperado el 14 de abril de 2012 de http://www.uria.com/documentos/publicaciones/1467/documento/art1.pdf?id=2064.

8 Vale la pena mencionar que el literal s, del artículo 5 del Real Reglamento (RDLOPD), que desarrolla la Ley Orgánica 15 del 13 de diciembre de 1999, Protección de Datos de Carácter Personal (LOPDCP), define la Transferencia Internacional de Datos como aquel "tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español"

9 Valga citar la Resolución 45/95 del 14 de diciembre de 1990 de la Asamblea General de la ONU que adoptó los "principios rectores para la reglamentación de los ficheros computadorizados de datos personales". Por ejemplo, en el principio denominado "Flujo de datos a través de las fronteras", se estableció: "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". Al anterior texto se suma la Guía para la protección de la

troductoria del artículo 12 del convenio citado se menciona que 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 a otro territorio de otra parte. Señala que cualquier parte tendrá la facultad de establecer una excepción en la medida en que su legislación prevé o prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación establezca una protección equivalente.

Al convenio se le une la Directiva 95/46/CE del Parlamento Europeo y el Consejo de la Unión Europea, de 24 de octubre de 1995. En el numeral 2 del artículo 26 de la directiva se establece que los Estados miembros podrán autorizar una o una serie de transferencias de datos personales a un tercer país que garantice un nivel de protección adecuado, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas.

Asimismo, el protocolo de la Decisión 2004/915/EC de la Comisión Europea dispone que "[con] el fin de facilitar los flujos de datos procedentes de la Comunidad, es conveniente que los responsables del tratamiento estén en condiciones de realizar transferencias de datos a escala mundial ateniéndose a un único conjunto de normas de protección de datos".

Igualmente, en la Propuesta de Reforma de la Directiva 95/46/CE[10], la Unión Europea insiste en que "los flujos transfronterizos de datos personales son necesarios para la expansión del comercio y la cooperación internacional". Sin embargo, en el proyecto se prohíbe de manera taxativa la transferencia a países que no garanticen un nivel adecuado de protección de datos (Numeral 78 de los considerandos), salvo que "el responsable o el encargado del tratamiento [adopte las] medidas para compensar la falta de protección de datos en un tercer país mediante las garantías apropiadas para el interesado". Considera como garantías apropiadas tales como: "Normas corporativas vinculantes", "Cláusulas tipo de protección de datos adopta-

privacidad y transferencia de flujos de información personal adoptada por la Organización para la Cooperación y el Desarrollo Económico (OCDE), de 23 de noviembre de1980, que indicó: "los países miembro deberían adoptar todas las medidas razonables y oportunas para garantizar la circulación transfronteriza, ininterrumpida y segura, de los datos personales, incluso el tránsito a través de algún país miembro" (numeral 16 III Parte). Señala que: "la circulación transfronteriza de datos personales entre dos países miembro no debería restringirse, salvo en el caso de que el país aún no haya observado sustancialmente esas Directrices o cuando la reexportación de tales datos soslayase su legislación nacional sobre la intimidad" (numeral 17 Parte III). Véase también el Protocolo Adicional de Convenio No. 108 para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, del 8 de noviembre de 2001, que indica: "Artículo 2- Transferencia de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio. 1. Cada Parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección". Por otra parte, téngase en cuenta que el Foro de Cooperación Económica Asia Pacifico (APEC), de noviembre de 2004, adoptó el "Marco de Privacidad de APEC, reconociendo la importancia de desarrollar protecciones efectivas para la privacidad que eviten barreras a los flujos de información, asegurar en intercambio continuo y el crecimiento económico en la región APEC" (Prólogo del Marco de privacidad del Foto de Cooperación Económica Asia Pacifica (APEC)).

10 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). Comisión Europea, Bruselas, enero 25 de 2012. En: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF. Se cita por algunos elementos que han sido propuestos en la reforma citada, y que el Gobierno Nacional debería considerar y abordar en la futura reglamentación de las NCV.

das por la Comisión", "Cláusulas tipo de protección de datos adoptadas por una autoridad de control" o "Cláusulas contractuales autorizadas por una autoridad de control" (Numeral 83 de los considerandos).

De tal forma, la Unión Europea se mantiene reticente a aceptar el flujo transfronterizo de datos personales con destino a países que no garanticen un "grado equiparable" de protección de datos al que se le ofrece a las personas de conformidad con las normas europeas. No se trata de limitar la libre circulación de datos, pues obsérvese que en la normatividad citada, se autoriza la transmisión cuando el exportador ofrezca las garantías adecuadas. La regulación sobre transferencias internacionales de datos tiene como objeto facilitar la exportación e importación de datos pero protegiendo los derechos y garantías de los titulares de la información interferidos en la administración de sus datos.

En el caso de Colombia, también existe la posición anotada anteriormente. Así, la Ley 1266 de 2008, Estatutaria de Hábeas Data[11], establece en el literal f, del artículo 5º[12], que regula el tema de la circulación de información, una serie de reglas sobre el flujo transfronterizo de datos. Dicha norma indica que "si el receptor de la información fuere un banco de datos extranjero, 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". Este literal fue declarado exequible por la Corte Constitucional, mediante sentencia C-1011 de 2008 M.P. Jaime Córdoba Triviño, en el sentido que el carácter adecuado del país de destino será evaluado por las Superintendencias de Industria y Comercio (SIC), y Financiera de Colombia (SFC), no por el operador nacional[13]. De acuerdo con este régimen, la transmisión internacional de datos quedó condicionada a que el banco de datos de destino ofrezca garantías suficientes para la protección de los derechos del titular, previa evaluación del ente de vigilancia y control.

Asimismo, la Ley 1581 de 2012". El párrafo quedaría así: Asimismo, la Ley 1581 de 2012, prohíbe la transferencia a países que no garanticen un nivel adecuado de protección de datos[14]. No

11 "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones". La Corte Constitucional, en el control previo de constitucionalidad de la Ley 1266 de 2008, sentencia C-1011 de 2008, aclaró que: "el Proyecto de Ley tiene un carácter sectorial, dirigido a la regulación de la administración de datos personales de contenido comercial, financiero y crediticio; por ende, la referencia realizada por el legislador estatutario al derecho a la información se circunscribe a ese carácter sectorial, y, en ese sentido, desvirtúa la posibilidad de interpretar la normatividad como una regulación integral de ese derecho".

12 "ART. 5º Circulación de información. 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".

13 El Alto Tribunal señaló que: "[la Superintendencia de Industria y Comercio, y la Superintendencia Financiera], 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".

14 La Corte Constitucional en la Sentencia C-748 de 2011 M.P. Jorge Ignacio Pretelt Chaljub, determinó que: "en un mundo globalizado en el que el flujo transfronterizo de datos es constante, la aplicación extraterritorial de los estándares de protección es indispensable para garantizar la protección adecuada de los datos personales de los residentes en Colombia, pues muchos de los tratamientos, en virtud de las nuevas tecnologías, ocurren precisamente fuera de las fronteras" M.P. Jorge Ignacio Pretelt Chaljub.

obstante, el legislador estatutario facultó a la Superintendencia de Industria y Comercio (SIC) a: "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 1°, artículo 26).

En ese sentido, en su Sentencia C-748 de 2011, la Corte Constitucional reiteró que la entidad encargada de establecer si otro país garantiza un nivel adecuado de protección de datos es la Superintendencia de Industria y Comercio. Asimismo, recalcó que: "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".

Es de considerar que por el acercamiento cada vez mayor al sistema normativo europeo, se ha incorporado en la legislación nacional y en la jurisprudencia constitucional el concepto de "nivel adecuado o equiparable de protección de datos", por lo que es indispensable estudiar qué se entiende por esta figura jurídica.

1. El concepto de nivel adecuado de protección de datos

El "nivel adecuado de protección de datos" es uno de los principios que rigen la transferencia internacional de datos, con el cual se busca que se garantice la protección de los derechos fundamentales de las personas en cuanto al procesamiento de sus datos personales. Para José Manuel Frutos, administrador principal de la Dirección General de Justicia, Libertad y Seguridad de la CE, "el dato no debe perder la protección por el simple hecho de que es exportado"(Agencia de Protección de Datos de la Comunidad de Madrid, 2008). Bajo la anterior premisa, Nelson Remolina (2010, p. 497), en "¿Tiene Colombia un nivel adecuado de protección de datos personales?", señala que: "la expresión 'adecuado' se refiere a que el Estado importador tenga un grado de protección superior, igual, similar o equivalente al del Estado exportador. Con lo anterior, se quiere impedir que con ocasión de una operación de exportación de datos personales se disminuya el nivel de protección que se le garantiza al titular del dato en el país exportador". En ese escenario, el citado autor reitera que lo que se busca es que en el flujo transfronterizo, el país de destino le otorgue al interesado los mismos derechos y garantías que se le ofrece en el país exportador, en cuanto la protección de su información personal. Esta regla es conocida como el "principio de continuidad de la protección de datos".

Hay que señalar que en la Unión Europea, el Grupo de Trabajo del artículo 29[15], en el Informe No. 12, aborda el tema relativo a lo que debe entenderse por "protección adecuada", y define los "principios de contenido"[16] y los "requisitos de procedimiento / de aplicación"[17], instaurados para asegurar que las normas aplicables resulten eficaces, y que ofrezcan en la práctica un verdadero cumplimiento en la protección a las personas cuyos datos son objetos de tratamiento (Grupo de Trabajo del Artículo 29, 1998). Por ello, no basta con que el país de destino consagre en su regulación el conjunto de principios relativos a la salvaguardia del derecho fundamental a la protección de datos personales, sino que se requiere que se cuente con herramientas legales y judiciales que garanticen la efectividad de las normas. Incluso, la existencia de autoridades de control que velen por el cumplimiento de las reglas por parte de la entidad exportadora e importadora (Matus, 2010, p. 4)[18].

Por otro lado, como se ha descrito anteriormente, el numeral 2 del artículo 26 de la Directiva 95/46/CE, permite la transferencia de datos personales cuando el responsable del tratamiento ofrezca las garantías necesarias "respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, incluyendo la eficacia del ejercicio de los respectivos derechos", independientemente de dónde estén almacenados, por ejemplo, las "Cláusulas Contractuales"[19].

15 Este Grupo de trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente sobre la protección de datos y la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

16 "I) Principios de contenido. Se sugiere la inclusión de los siguientes principios básicos: 1) Principio de limitación de objetivos; 2) Principio de proporcionalidad y de calidad de los datos; 3) Principio de transparencia; 4) Principio de seguridad; 5) Derechos de acceso, rectificación y oposición; 6) Restricciones respecto a transferencias sucesivas a otros terceros países (...)".

17 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); 2) Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos; y, 3) Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

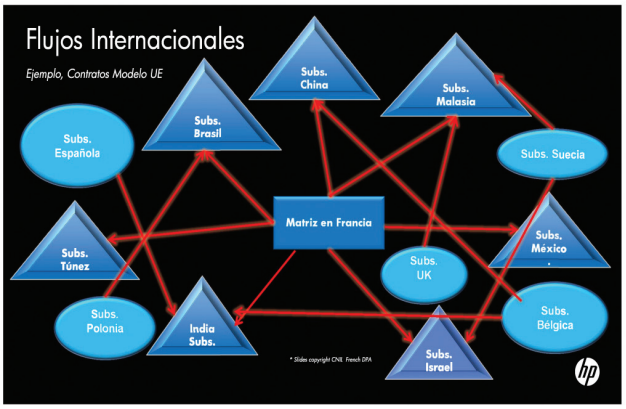
18 Según Jessica Matus Arenas define el concepto de "protección adecuada", en primer término, a que los terceros países deben garantizar el conjunto de principios básicos de protección de datos contenido en la Directiva Europea, y garantizar dichos principios de una manera efectiva, por ello, como se ha expresado, no basta la sola legislación que plasme estos principios, sino que se establezcan los medios idóneos para ejercitar estos derechos, esto es, que exista un órgano de control responsable de la protección de datos no sólo autónomo sino independiente, con un campo de aplicación amplio, esto es, público y privado, facultades de fiscalización y sancionadoras, un catálogo de infracciones y sanciones que sean disuasivas para los responsables de bancos de datos, acciones administrativas y/o judiciales, medidas de seguridad, la promoción de los derechos de los titulares de datos y de las obligaciones respecto de los bancos de datos, disponer de sistemas de responsabilidad y reparación para los afectados cuando no se de cumplimiento a las normas establecidas".

El numeral 2 del artículo 25 de la Directiva 95/46/CE, define que: "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".

19 Este mecanismo, como ya se anotó, ha sido regulado en la Unión Europea en la Directiva 95/46/CE y han sido desarrollados por: (i) Decisión 2001/497/CE, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país. VERSIÓN CONSOLIDADA de la Decisión 2001/497/CE, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país; (ii) Decisión 2004/915/CE, de 27 de diciembre de 2004 , por la que se modifica la Decisión 2001/497/CE, de 15 de junio de 2001; (iii) Decisión 2002/16/CE, de 27 de diciembre de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países (queda derogada a partir de 15 de mayo de 2010); (iv) Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Ver Remolina (2010, pp. 386-403).

No es el objeto de este documento hacer un análisis exhaustivo de los componentes de las "Cláusulas Contractuales". Basta, pues, mencionar que mediante esta figura jurídica el exportador e importador se obligan contractualmente a garantizar eficazmente el respeto de la protección de los datos de los titulares por cada transferencia que se realice. Así, si una empresa ubicada en Francia quiere transferir los datos de sus clientes a un *call center* ubicado en Guatemala, puede realizarlo a través de la vía contractual. Sin embargo, como se puede observar en la siguiente imagen, el flujo transfronterizo a través de "cláusulas contractuales" prevé un costo económico y jurídico para el responsable, pues requiere que por cada una de las operaciones, se requiera acudir a la celebración de un contrato con el responsable[20] o encargado[21] del tratamiento. Adicionalmente, cada contrato debe ser evaluado por la Autoridad de Control del país exportador lo cual demora, en promedio, tres meses como sucede en España.

Figura 2. Problema que se genera para un grupo corporativo al momento de trasferir los datos de personales a las filiales o sucursales a través de múltiples cláusulas contractuales.



Fuente: Hewlett-Packard Development Company: 2011

El aspecto más relevante que se ha puesto de manifiesto en el presente capítulo es la posibilidad de que el responsable del tratamiento ofrezca las garantías suficientes para que se legalice la transferencia de datos personales a destinos que no aseguren un nivel equiparable de protección. Este hecho genera que las empresas requieran de políticas globales mediante esquemas de "autorregulación" o "autoevalua-

20 El Proyecto de Ley del Senado Número 184 y 046 de la Cámara del 2010 (hoy Ley 1581 de 2012), define al responsable del tratamiento como aquella "[p]ersona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos" (literal e, del articulo 3). Para la Corte Constitucional, en la sentencia de constitucionalidad del proyecto de ley, "el concepto de responsable puede cobijar tanto a la fuente como al usuario, en los casos en los que dichos agentes tengan la posibilidad de decidir sobre las finalidades del tratamiento y los medios empleados para el efecto, por ejemplo, para ponerlo en circulación o usarlo de alguna manera". Estableció que: "los responsables del tratamiento tienen mayores compromisos y deberes frente al titular del dato, pues son los llamados a garantizar en primer lugar el derecho fundamental al hábeas data, así como las condiciones de seguridad para impedir cualquier tratamiento ilícito del dato".

La Directiva 95/46/CE, dispone que "[el] responsable del tratamiento [es] la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos, personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario" (literal d, artículo 2).

21 El Proyecto de Ley del Senado Número 184 y 046 de la Cámara del 2010 (hoy Ley 1581 de 2012), define al encargado del tratamiento como aquella "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". (literal d, del artículo 3). Para el Alto Tribunal Constitucional, en la sentencia de constitucionalidad de la Ley, "el criterio de delegación coincide con el término "por cuenta de" utilizado por el literal [d)], lo que da a entender una relación de subordinación del encargado al responsable". Indicó que: "el encargado del tratamiento no puede ser el mismo responsable, pues se requiere que existan dos personas identificables e independientes, natural y jurídicamente, entre las cuales una –el responsable– le señala a la otra –el encargado– como quiere el procesamiento de unos determinados datos. En este orden, el encargado recibe unas instrucciones sobre las forma como los datos serán administrados". La Directiva 95/46/CE, dispone que "[el] encargado del tratamiento [es] la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento" (literal e, artículo 2).

ción" que permitan garantizar a los ciudadanos los mismos derechos y garantías consagradas en la normatividad del país exportador.

B. Los sistemas de "autorregulación"

Los mecanismos de "autorregulación" son una institución jurídica que ha tenido consagración en los marcos regulatorios sobre protección de datos personales en algunos países, entre los que se encuentran a título enunciativo no explicativo, Argentina, Costa Rica, México y Perú, en la medida en que, por una parte, los responsables en el tratamiento de los datos personales adoptan, de manera unilateral, una serie de instrumentos propios encaminados a garantizar el respeto de los derechos fundamentales de los titulares, en la recolección, almacenamiento, circulación, publicación y uso que se le dé a su información personal; de tal forma que no se pongan en peligro o se lesionen los derechos fundamentales de los titulares[22]. Por otra parte, "[los Estados garantizan] un nivel mínimo de protección a los ciudadanos frente al tratamiento de sus datos personales" (Remolina, 2010, p. 368). Y finalmente, como lo señala Alejandra Castro Bonilla, "la ["autorregulación"] por ende [es un sistema basado en la competencia]" (uned.ac.cr.com:2, 2003).

A nivel de la Unión Europea se tiene, por ejemplo, en primer lugar, el artículo 27 de la Directiva 95/46/CE del Parlamento Europeo y el Consejo de la Unión Europea, que establece: "Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros". Sin embargo, se puede observar que en la norma se recalca que: "[los] proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales"[23].

En segundo lugar, otro punto de referencia a nivel Europeo, es el Informe No. 07, en el cual el Grupo de Trabajo del artículo 29, definió el concepto de "autorregulación", como "cualquier conjunto de normas de protección de datos que se apliquen a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión". Para el Grupo de Trabajo (1998, pp. 1-10) es necesario que un sistema de autorregulación no solo refleje los principios básicos necesarios para la protección de datos sino que

22 Fernando Barrio (2006, p. 129), citando a Aguilar J, señala que: "la autorregulación aumenta los niveles de protección al consumidor debido a que las empresas tienen un especial interés en hacer cumplir sus políticas de privacidad". Alberto Cerda Silva (2006), en "Algunas consideraciones sobre los códigos de conducta en la protección de los datos personales", en relación a los sistemas de "autorregulación", indica que "se veía en ellos no solo un medio para hacer frente al desfase normativo y, a la vez, concretar la aplicación de sus disposiciones a circunstancias específicas. Ver también Alberto Cerda Silva (2008, pp. 121-130) en "Hacia un modelo integrado de regulación y control en la protección de los datos personales". Resulta trascendental no dejar de mencionar, así sea someramente, que la Organización para la Cooperación y el Desarrollo Económico (OECD), reitera la necesidad de "fomentar y apoyar la autorregulación, ya sea en forma de códigos de conducta o de otro modo" (literal b, del artículo 19 de la IV Parte de las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales, de 23 de noviembre de 1980).

23 Fernando Barrio (2006, p. 129) señala que "sin la intervención gubernamental las empresas no tendrían motivos para diseñar políticas beneficiarias para los usuarios, pudiendo dar lugar a fraudes y otras violaciones de los derechos del consumidor".

efectivamente garantice un nivel satisfactorio de cumplimiento del sistema de autorregulación a través de sanciones disciplinarias o pecuniarias, se proporcione un apoyo y ayuda institucional imparcial, independiente y de fácil acceso para los individuos cuyos datos sean objeto de tratamiento. Asimismo, recalca la necesidad que "[tenga el carácter vinculante] para todos los miembros a quien se transfieren los datos personales y se proporcione una protección adecuada si los datos se transfieren a terceros".

Otro documento a analizar son los Estándares Internacionales sobre Protección de Datos Personales y Privacidad –de ahora en adelante Resolución de Madrid (2009)–, en la que establece como una medida proactiva[24],"la adhesión a acuerdos de autorregulación cuya observancia resulte vinculante, que contengan elementos que permitan medir sus niveles de eficacia en cuanto al cumplimiento y grado de protección de los datos de carácter personal, y establezcan medidas efectivas en caso de incumplimiento" (literal g, del estándar internacional número 22).

De esta manera, explica Nelson Remolina (2010, pp. 368-369) que el modelo de regulación europeo "se nutre de un plexo jurídico conformado por normas generales sectoriales, aunadas a la existencia de una autoridad de control que vele por el cumplimiento de la regulación", a diferencia del sistema de regulación de la protección de datos personales norteamericano en el que "[no se considera] esencial la existencia de un organismo de supervisión (agencias de protección de datos). Prefieren la autorregulación y la promulgación de varias normas sectoriales en lugar de disposiciones generales". De tal forma, en uno u otro caso, se busca que el responsable y encargado del tratamiento cumplan con el conjunto de principios que regulan el procedimiento de la información personal.

En este mismo punto resulta trascendental no dejar de mencionar los diferentes informes que se han acogido en los respectivos encuentros que ha realizado la Red Iberoamericana de Protección de Datos y el documento que ha presentado el Grupo de Trabajo sobre Autorregulación Temporal y Protección de Datos Personales, en los cuales se ha señalado la posibilidad de que el responsable del tratamiento adopte sus propias herramientas con el objetivo de fomentar la confianza y seguridad en la libre circulación de los datos personales en las redes globales. Dentro de los documentos se puede mencionar las siguientes conclusiones:

- En el III Encuentro Iberoamericano de Protección de Datos (2004, pp. 3-5) celebrado en la ciudad de Cartagena de Indias, Colombia, se avaló la creación de mecanismos de autorregulación, complementarios a los marcos regulatorios, en el sector de las telecomunicaciones e internet.

- En el IV Encuentro Iberoamericano de Protección de Datos (2005, pp.4-6) celebrado en la Ciudad de México y en Huixquilucan, se recalcó la implicación que la protección de datos supone en otros ámbitos de la actividad económi-

24 "Estándar Internacional No. 22. Los Estados incentivarán, a través de su derecho interno, el establecimiento por quienes intervengan en cualquier fase del tratamiento de medidas que promuevan el mejor cumplimiento de la legislación que resulte aplicable en materia de protección de datos. Entre dichas medidas podrán encontrarse, entre otras".

ca como lo son, entre otras, las transferencias internacionales de datos como elemento imprescindible para el desarrollo del comercio en mercados regionales o en el mercado mundial. Otro punto importante que se discutió es la existencia de iniciativas de los propios operadores para que la protección de los datos personales se lleven a cabo a través de instrumentos de autorregulación. Se señaló que estos mecanismos permiten adoptar la normativa a las especificadas que presenta el tratamiento de datos en un determinado sector, de forma que se generen estándares a las necesidades del sector, que faciliten su cumplimiento. Sin embargo, se aclaró que estas herramientas deben tener la categoría de carácter complementario a un marco normativo previamente definido por el Estado.

- El Grupo de Trabajo sobre autorregulación temporal y protección de datos personales en lo que respecta a las herramientas de autorregulación (2006, pp. 6-9), consideró, entre otras, que estas herramientas "no solo contribuye[n] a consolidar una cultura de protección [del derecho fundamental de hábeas data] sino que fomenta y consolida el correcto tratamiento sobre las personas"[25]. El informe avala la necesidad que estos mecanismos tengan un carácter vinculante a través, entre otros[26], de sistemas de control interno y externo de verificación del cumplimiento de los códigos, mediante los cuales se permita determinar el verdadero grado de contribución de los instrumentos de autorregulación a la protección de los datos personales. No debe perderse de vista que el Grupo de Trabajo reitera en que estas herramientas no sustituyen "la imprescindible gestión y responsabilidad de los Estados en reconocer y garantizar de manera efectiva la tutela del derecho fundamental de la protección de datos personales"[27], enfoque que en alguna medida es seguido en nuestro país, como se explicará a continuación:

En efecto, en nuestra legislación, la Ley 1266 de 2008, Estatutaria de Hábeas Data[28], da los

25 Es importante que los responsables de tratamiento de datos personales creen instrumentos de autorregulación por las siguientes razones: (1) Representa una manifestación positiva de la responsabilidad social de las empresas de garantizar los derechos fundamentales creando mecanismos que otorgan garantías o beneficios adicionales en relación con lo dispuesto en los marcos regulatorios; (2) La debida implementación de los instrumentos de autorregulación facilita el cumplimiento de los principios de protección de datos y eleva los estándares de calidad en este ámbito; (3) El correcto tratamiento de los datos personales genera confianza en las personas y facilita el intercambio de información; (4) Se ha evidenciado la tendencia de las personas de preferir realizar negocios o actividades con empresas que garantizan niveles altos de protección de datos personales; (5) La existencia y aplicación de códigos de conducta puede representar una ventaja competitiva de las empresas en la medida que este es un factor que las personas tienen en cuenta a la hora de realizar actividades con terceros; (6) Las empresas pueden posicionar e incrementar su buen nombre y confianza dentro de su clientela y la sociedad en general al evidenciar su interés y compromiso con la protección de los datos personales.

26 En virtud de lo anterior resulta imprescindible que los instrumentos de autorregulación estén acompañados de herramientas que los hagan eficaces. Dentro de estos mecanismos se sugieren los siguientes: (1) Establecer medios ágiles, efectivos y gratuitos en caso de inobservancia del código para que la persona no solo exija el respeto de sus derechos y libertades sino que se convierta en un "fiscalizador" de la gestión del administrador de sus datos personales (2) Consagrar mecanismos de control interno y externo de verificación del cumplimiento de los códigos, y (3) Prever sanciones por el incumplimiento de los códigos.

27 Finalmente, el Grupo de Trabajo recapitulo sus apreciaciones en las siguientes recomendaciones: 1. Incorporar en las futuras regulaciones disposiciones explícitas tendentes a utilizar mecanismos de autorregulación que: (a) Representen un valor añadido en su contenido respecto de lo dispuesto en las leyes, y (b) Contengan o estén acompañados de mecanismos que permitan medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales; 2. Concebir la autorregulación como un mecanismo no sustituto ni suficiente para garantizar la protección de los datos personales y como una herramienta complementaria al marco legal para fomentar la cultura de tutela de los datos personales; 3. Consagrar medidas efectivas en caso de incumplimiento de los instrumentos de autorregulación; 4. Promover mecanismos de publicidad de los instrumentos de autorregulación, con especial consideración a la existencia de registros públicos.

28 "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos

primeros pasos hacía la adopción de instrumentos de autorregulación. El numeral 4, del artículo 7º obliga al operador de la información a: "adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares"[29]. Sin embargo, se ve que la norma estatutaria, a diferencia de la Directiva 95/46/CE, no prevé que los manuales internos sean sometidos a un análisis previo y a un aval por parte de la Superintendencia de Industria y Comercio[30], respecto de su adecuación a la medida regulatoria,[31] generando posiblemente un abuso de la facultad informática de las empresas tanto en el diseño como en la implementación de los códigos de conducta.

Se concluye que la "autorregulación" es un instrumento que genera "un valor añadido" en el tratamiento de los datos personales, pues el responsable del proceso de manera voluntaria incorpora en sus códigos internos unas garantías adicionales a las previstas en la normatividad de protección de datos, a saber, agilidad en el trámite de las consultas y quejas, consolida una cultura de protección de datos, genera confianza en las empresas, vías adecuadas de reparación a quienes resulten perjudicados en sus derechos. Asimismo, se parte de la base que las entidades que se adhieren a un sistema de "autorregulación", quedan vinculadas de manera obligatoria a su cumplimiento, de tal forma que su inobservancia acarrea las sanciones pertinentes para los infractores. En efecto, como lo reitera el Grupo de Trabajo de la Red Iberoamericana de Protección de Datos (2006, p. 8) "[este sistema no se puede constituir] en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales".

Las anteriores apreciaciones nos permiten entender que las NCV son un sistema de "autorregulación", que ofrece las garantías necesarias de respeto y protección de los derechos de los titulares de los datos en el movimiento transfronterizo de información personal, siempre y cuando, estas efectivamente se cumplan y respeten.

personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

29 La Corte Constitucional en la Sentencia C-1011 de 2008 M.P. Jaime Córdoba Triviño, indicó que: "la exigencia de adopción de un manual interno de políticas y procedimientos, en los términos de la norma analizada, es una disposición destinada a otorgar transparencia a la gestión de la información de las personas, en la medida en que permite consignar en instrumentos prescriptivos de las entidades el mecanismo para efectivizar los derechos de los titulares".

30 ART. 17.—Función de vigilancia.<Artículo CONDICIONALMENTE exequible> La Superintendencia de Industria y Comercio ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula en la presente ley.

31 Valga citar también, la postura de Raúl Arrieta Cortés (2011, p. 5) en "Autorregulación y protección de datos personales", en el que considera que: "para que la autorregulación realmente sea útil y confiable estimamos que resulta indispensable que sea el propio Estado el que regule el contexto de ésta, lo que supone, por un lado el establecimiento de sistemas de control de la misma y, por otro, la fijación legal o reglamentaria"..

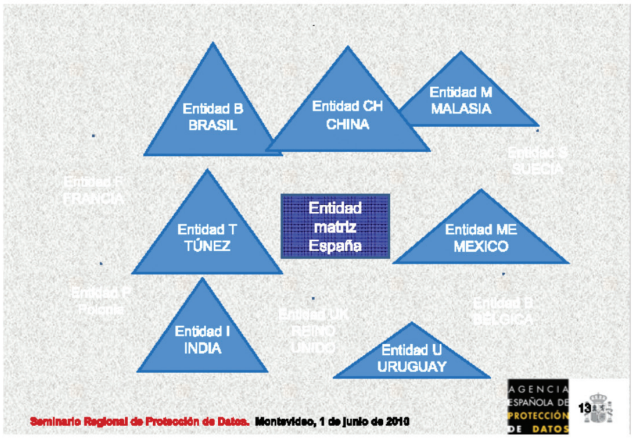
II. ESTABLECIMIENTOS DE GARANTÍAS ADECUADAS: NORMAS CORPORATIVAS VINCULANTES

En el capítulo anterior se describe el progresivo desarrollo normativo en el tratamiento de datos personales de la Unión Europea[32], encaminado a facilitar el comercio a escala global, y a su vez proteger los derechos y garantías de las personas, y que ha permitido crear un ambiente favorable para la adopción e implementación de mecanismos de autorregulación en el seno de grupos corporativos, a saber las NCV. Para el efecto es preciso estudiar la estructura jurídica de esta herramienta.

A. Concepto

Como fue señalado al iniciar el presente escrito, las empresas necesitan aplicar estándares, estrategias y procedimientos uniformes que fomenten y garanticen un alto nivel de protección en el tratamiento y procesamiento de los datos personales, especialmente, cuando el país de destino de la transferencia no garantiza un nivel adecuado de seguridad en la protección de los mismos, buscando que la información fluya sin trabas regulatorias a nivel mundial. La siguiente gráfica evidencia cómo, en la práctica, circulan libremente las fichas de los sujetos en el seno de un grupo corporativo no viendo la necesidad de acudir por cada transferencia a la vía contractual (cláusulas contractuales) (Blanco, 2010 p. 14).

Figura 3. Flujo transfronterizo de datos en un grupo corporativo sin que se requiera acudir por cada una de las operaciones a las claususlas contratuales.



Fuente: Agencia Española de Protección de Datos, 2010

Las NCV son un "código de prácticas" en materia de tratamiento de datos personales, que los grupos empresariales han adoptado e incorporado a su funcionamiento interno, con la finalidad de facilitar las transferencias internacionales dentro de su organización. Las NCV son un mecanismo adecuado que permite la transmisión de información de los titulares a países que no garantizan un nivel "adecuado" o "equiparable" de protección de datos. Se trata, por tanto, de una forma de avalar la libre circulación de información sin poner en peligro el nivel de protección de datos de los sujetos previsto en el país exportador.

Tenemos que, de una parte, la compañía multinacional se obliga a un procedimiento conjunto en el tratamiento de los datos personales dentro de su organización, las incorpora a su funcionamiento y las sigue de manera voluntaria. En

32 Vale la pena reiterar que este tema en Colombia solo se reguló a propósito del Proyecto de Ley del Senado Número 184 y 046 de la Cámara del 2010 (hoy Ley 1581 de 2012). En esa medida, a excepción de los principios generales en materia de protección de los datos, hemos considerado abordar la normatividad europea para el desarrollo del presente capítulo, consideramos a título personal que el origen de las NCV deviene de ella.

esa línea de análisis, Frédéric Blas (2009, p. 52) señala que: "[el concepto de las "NCV"] es algo peculiar: una compañía se hace una promesa a sí misma, o sus filiales o su casa matriz: la de respetar la política [intracorporativa] de protección de datos". Por otra parte, permite la libre circulación de los datos hacia países que carecen de legislación en la materia o donde esta es mínima.

1. Las NCV en la Unión Europea

Para Susan Chen Sui (2008, p. 225) "las [NCV] son un instrumento permitido por la Unión Europea, que flexibiliza [o simplifica el trámite regulatorio en] los movimientos internacionales de datos personales entre un grupo de empresas multinacionales con filiales establecidas incluso fuera del espacio económico Europeo. Es un nuevo mecanismo válido para legitimar las transferencias de datos personales entre empresas de un mismo grupo". Así, a nivel de la Unión Europea vemos que el concepto y procedimiento para la aprobación de las NCV, se encuentran expuestos en los diferentes documentos del Grupo de Trabajo del artículo 29, informes que serán desglosados para explicar el alcance de las NCV y que, a su vez, son un insumo relevante para considerar en la futura reglamentación de las mismas en Colombia. A continuación unas cuestiones básicas sobre los instrumentos.

a. En el Documento Número 74, el Grupo de Trabajo expone la naturaleza jurídica de las NCV, entre otras, establece que se deben aplicar en todo el grupo corporativo, independiente del lugar donde se encuentra ubicado el miembro; resalta el carácter vinculante o de exigibilidad jurídica de las reglas; indica que las políticas deben ser claras, precisas, y que permitan ser una verdadera garantía en la transferencia de datos a terceros países; define la noción de grupo empresarial; resalta la colaboración entre el grupo corporativo y las agencias de protección de datos; aclara que las normas corporativas no pueden sustituir las responsabilidades por los cuales los responsables o encargados del tratamiento están obligados por ley; y, recalca que los principios rectores en materia de protección de datos personales deben estar incorporados en las normas corporativas (Grupo de Trabajo del Artículo 29, 2003).

b. En el Documento Número 107, el grupo de trabajo fijó un procedimiento para la competencia y colaboración de las autoridades de protección de datos a nivel europeo para la aprobación de las NCV (Grupo de Trabajo del Artículo 29, 2005).

c. El Documento Número 108 establece un modelo de solicitud de aprobación de normas internas vinculantes y que ofrezcan efectivamente las garantías adecuadas de protección (Grupo de Trabajo del Artículo 29, 2005).

d. El Documento Número 153 expone de forma detallada los elementos y principios que se deben contener en las NCV (Grupo de Trabajo del Artículo 29, 2008).

e. El Documento Número 154, establece la estructura de las NCV (Grupo de Trabajo del Artículo 29, 2008).

f. El Informe de Trabajo Número 155 resuelve interrogantes sobre el alcance jurídico de las NCV (Grupo de Trabajo del Artículo 29, 2009).

Estos informes de trabajo son consistentes con la propuesta de reforma de la Directiva 95/46/CE, que introduce de manera explícita el concepto de las NCV como una garantía apropiada de la protección de datos (Numeral 82 de los considerandos). Por lo que respecta a su definición, la propuesta señala en el numeral 17 del artículo 4º que las NCV son un conjunto "[de] políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro de la Unión para las transferencias o un conjunto de transferencias de datos personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un grupo de empresas".

La propuesta de reforma planteada por la Comisión Europea contempla que: "todo grupo de sociedades debe poder hacer uso de normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo de empresas, siempre que tales normas corporativas incluyan principios esenciales y derechos aplicables con el fin de asegurar las garantías apropiadas para las transferencias o categorías de transferencias de datos de carácter personal" (Numeral 85 de los considerandos).

En conclusión, se puede afirmar que la aproximación normativa descrita corresponde a una categoría de herramientas legales que permiten compensar la falta de protección de datos en un tercer país ubicado por fuera de la Unión Europea a través de la creación de una "política de privacidad interna" del grupo empresarial.

B. Elementos Esenciales de las NCV

En el Informe de Trabajo No. 74, el Grupo de Trabajo retoma dos elementos esenciales en el análisis de las NCV. El primero, orientado a determinar el alcance de la obligatoriedad de las reglas corporativas como política de privacidad interna. El segundo, enfocado a definir el carácter jurídicamente vinculante frente a los miembros del grupo empresarial, como frente a terceros. Asimismo, contemplamos la existencia de un tercer elemento encaminado a delimitar el campo de aplicación de las NCV.

1. Carácter obligatorio

Tenemos que las NCV deben implementarse correctamente y cumplirse a nivel multinacional, regla que aplica a todas las partes integrantes de la organización, incluidos sus empleados y contratistas (obligatoriedad interna). Lo que permite indicar que las personas que intervienen en la transferencia de datos deben estar en capacidad de conocerlas, entenderlas y aplicarlas. No hay que olvidar que las NCV están desarrolladas en los códigos de conductas[33] adoptados por el grupo multinacional.

33 Un código de conducta puede llegar a ser una NCV, si cumple los requisitos que señalamos en este texto; pero no todo código de conducta es, perse, NCV.

Federico Carnikian (2010, p. 27) señala que este tipo de reglas a cumplir pueden estar recogidas en otros Códigos de Conducta perteneciente al grupo de empresas que coadyuven al fortalecimiento del cumplimiento de la normativa de protección de datos personales. A vía de ejemplo, aquellos que contengan normas relativas a las medidas de seguridad para la protección de datos, deber de confidencialidad, etc.

Así las cosas, una de las principales responsabilidades del grupo multinacional es velar por el cumplimiento de su pólitica colectiva dentro su organización. Por consiguiente, cuando se quebrante alguna de las normas contempladas en el cuerpo de las NCV, a nivel interno, se pueden adoptar sanciones disciplinarias, y a nivel externo, da lugar a reparar los daños causados[34].

2. Carácter vinculante

El Grupo de Trabajo en el informe número 74 señala que el carácter vinculante de las NCV, en la práctica, implica, por una parte, que los miembros del grupo empresarial, así como cada empleado, se sientan obligados a cumplir con las normas internas. Como se mencionó anteriormente, las NCV deben contemplar la existencia de medidas sancionatorias en caso de violación de las mismas. Asimismo, se requiere adoptar dispositivos de capacitación para los empleados y subcontratistas, propiciando una educación especial en la formación de protección de datos (carácter jurídicamente vinculante a nivel interno). Por otra parte, surge el derecho del sujeto del dato a exigir el cumplimiento de las normas ante las autoridades de protección de datos o por la vía judicial, (carácter jurídicamente vinculante a nivel externo). Como lo resalta el profesor Federico Carnikian (2010, p. 27) "un aspecto relevante a destacar, es que las [NCV] deben ser vinculantes legalmente dentro y fuera del grupo".

Igualmente, en el Informe de Trabajo Número 108 se indica que los empleados deben regirse por las NCV, a través de obligaciones específicas que figuran en sus contratos laborales que, a su vez, suponen una vinculación y observancia de las reglas y los procedimientos disciplinarios.

El documento introduce una serie de ejemplos de cómo las NCV pueden ser aceptables en una organización. En primer lugar, indica que una vez la matriz adopte las reglas corporativas, las mismas se hacen efectivas para los demás miembros del grupo. En segundo lugar, trae a colación la necesidad de adoptar un manual de deberes y medidas coercitivas redactadas en códigos de conducta. En tercer lugar, señala que deben estar incorporadas dentro de los principios generales de la empresa, respaldada por unas políticas claras y transparentes, mediante el monitoreo constante de sistemas de auditorías internas, externas o mixtas, y la adopción un sistema sancionatorio. Finalmente, recalca que el cumplimiento de las normas dependerá de la estructura y tamaño de la organización.

Hay que tener en cuenta que en el informe se reitera que las reglas deben ser vinculantes tan-

34 Muestra de ello es que en la Propuesta de Reforma de la Directiva 95/46/CE, se señala que las NCV especificaran que: "[el derecho del interesado] a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes", (literal e, del artículo 43) y " los mecanismos establecidos dentro del grupo de empresas para garantizar que se verifica el cumplimiento de las normas corporativas vinculantes" (literal i, del artículo citado).

to en la organización como a nivel externo para el beneficio de las personas. En efecto, el empleado que no respete los compromisos adoptados en las NCV se verá expuesto a medidas coercitivas, incluida la suspensión temporal de sus labores o la terminación definitiva de su contrato.

Por ejemplo, el 2 de noviembre de 2009, la entidad de *eBay*, estableció en sus NCV que: "las reglas corporativas tienen un carácter vinculante y el empleado que no las siga se verá **expuesto a medidas correctivas, incluida la rescisión de su contrato y otras sanciones conforme a la ley**"[35]. Otro ejemplo, es la decisión en la cual la Agencia Española de Protección de Datos (2009, p. 9), resolvió la solicitud de autorización de transferencia de datos de General Electric. En dicha aprobación, la autoridad de protección de datos señaló que: "la obligación de quienes traten los datos de cumplir con los principios y obligaciones contenidos en las [NCV], debiendo poderse adoptar asimismo medidas coercitivas en caso de que quede acreditado el incumplimiento por alguna de esas personas".

En este punto surge la siguiente pregunta ¿a partir de qué momento adquieren el carácter vinculante las NCV?

A nivel externo, la Propuesta de Reforma de la Directiva 95/46/CE, resuelve el interrogante, pues establece que: "[la] autoridad de control aprobará [las] normas corporativas vinculantes". En esa medida, a partir del momento en que cualquier autoridad de protección de datos de la Unión Europea autoriza las NCV, estas adquieren la calidad de vinculantes para las terceras personas, quienes a su vez tienen derecho a exigir el cumplimiento de las normas ante la Agencia de Protección de Datos o por la vía judicial[36]. Ahora bien, a nivel interno, se piensa que no hay problema en la interpretación de las normas, pues se adquiere cuando el grupo empresarial lo incorpora voluntariamente como política de privacidad interna en el conglomerado corporativo.

Las NCV implican un compromiso real de los miembros del grupo, mediante la adopción de procedimientos y medidas necesarias, por ejemplo, sanciones disciplinarias que permitan demostrar, entre otras, que existen las suficientes garantías. Asimismo, es responsabilidad del grupo empresarial garantizar que todos sus miembros tengan un conocimiento pleno y efectivo de las NCV.

3. Grupo empresarial

De acuerdo con lo expuesto en el Informe de Trabajo Número 74, las NCV, se halla limitada a que los grupos multinacionales se encuentren vinculados por unas reglas comunes de protección de datos. El Documento de Trabajo entiende como "grupo empresarial" aquel conjunto de empresas que son efectivamente obligadas por las normas. Define que el "grupo empresarial" puede variar de un país a otro y pueden corresponder a unas realidades empresariales

35 Negrillas fuera del texto original.

36 Rosa Barceló y María Verónica Pérez Asinare (2008, p. 164) han señalado que: "la autorización de la Agencia dará lugar a que dichas normas sean vinculantes".

muy diferentes, desde un conjunto, una jerarquía estructurada, grupos de conglomerados sueltos, grupo de empresas que comporten actividades económicas muy similares o muy diferentes. Como se señala el numeral 3.3 del informe número 74, el carácter obligatorio y coercitivo de las normas corporativas es el elemento que debe estar presente en todos los sistemas de transferencia de datos a terceros países.

En la propuesta de reforma de la Directiva 95/46/CE se establece que: "un grupo de empresas debe estar constituido por una empresa que ejerce el control y las empresas controladas, en virtud de lo cual la empresa que ejerce el control debe ser la empresa que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, las normas que la rigen o el poder de hacer que se cumplan las normas de protección de datos personales" (Numeral 28 de los considerandos). Bajo el anterior concepto queda prohibida la transferencia de datos a otras sociedades que no hagan parte del mismo grupo corporativo.

En todo caso, surge la necesidad que las normas corporativas vinculen y obliguen a otras personas que no hacen parte de la multinacional a lo dispuesto en las NCV, a manera de ejemplo, los *call center*, que en muchos casos, son vinculados a través de subcontratos[37]. En el Informe de Trabajo Número 74, el Grupo de Trabajo soluciona el anterior interrogante mediante la suscripción de cláusulas contractuales tipo aprobadas por la Comisión Europea.

C. *Contenido de las NCV*

En el Documento de Trabajo Número 74, se establece que las NCV deben adoptar un nivel razonable de detalle en la descripción de los datos, flujos y cumplir con la finalidad del tratamiento de la información de los sujetos. Para Susan Chen (2008, p. 226) "las NCV [deben describir] con suficiente detalle el flujo de datos, propósitos del procesamiento, personal encargado, actividad económica perseguida, etc., que permitan asegurar que el tratamiento de los datos es adecuado". En esa medida, en los diferentes informes de trabajo y en la Propuesta de Reforma de la Directiva 95/46/CE, las reglas corporativas especificarán como mínimo, entre otras[38], la siguiente información.

1. Principios generales

Para analizar el contenido de las NCV, es preciso tener en cuenta que el grupo multinacional debe garantizar su sometimiento a los principios y a las legislaciones nacionales en materia de protección de datos. La doctrina presentada por Valverde (2009, p. 8) señala que "[los] principios *per se* resultan excesivamente teóricos y aportan muy poco a las industrias implicadas, además deben ser desarrollados de forma que puedan ser aplicados de una manera realista y práctica a los tratamientos que lleven a cabo las

37 Señala Emilio del Peso Navarro et ál. (2008, p. 83) que "desde un principio, la subcontratación de trabajo no ha tenido una buena acogida por los rectores de la protección de datos y entendemos que esto ha sido así por no haberlo comprendido en todas sus dimensiones y por parecer ignorar su implantación en el tráfico empresarial".

38 Valga también citar el numeral 2, del artículo 43 de la Propuesta de Reforma de la Directiva 95/46/CE.

empresas de una manera que permita su compresión y aplicación efectiva por aquellos que tengan responsabilidades sobre protección de datos en la organización". En todo caso, la adopción de los principios es, sin duda, la principal guía para evaluar si el grupo multinacional ofrece garantías adecuadas de protección de datos.

Además, a la vista del Informe de Trabajo Número 74, se puede observar que los criterios de protección contenidos en las NCV deben cumplir con los estándares establecidos en la Directiva 95/46 CE y en el Documento de Trabajo Número 12, entre los que se encuentran: (i) principio de limitación de objetivos; (ii) principio de proporcionalidad y de calidad de los datos; (iii) principio de transparencia; (iv) principio de seguridad; y, (v) principio de acceso, rectificación y oposición. Así, es preciso señalar que el artículo 29 insiste en la necesidad de la adopción de unos principios objetivos que permitan determinar si una empresa multinacional es respetuosa o no del derecho fundamental de los datos personales.[39]

En Colombia, los principios rectores para el tratamiento de datos personales se encuentran incorporados en la Ley 1266 de 2008[40] y en la Ley 1581 de 2012[41]. El primer principio contemplado, valga la redundancia, en la Ley 1266 de 2008, pretende garantizar la veracidad o calidad de los registros o datos: señala la norma que la información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Está prohibido el registro y divulgación de datos falsos, erróneos, inexactos, incompletos o fraccionados.

En cuanto el principio de confidencialidad, el literal g, del artículo 4º, señala que: "todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligados a garantizar la reserva de la información inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, realizando suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma". El principio va encaminado a garantizar que la política de administración de datos sea conoci-

39 Se recalca, para efectos de constatar la importancia de los principios en materia de protección de datos, que el Marco de Privacidad aprobado por el Foro de Cooperación Económica Asía Pacífica (APEC), de noviembre de 2004, consagra, a título enunciativo, los siguientes principios de privacidad de la información: (i) Previniendo Daño; (ii) Aviso; (iii) Limitación de Recolección; (iv) Uso de la Información Personal; (v) Elección; (vi) Integridad de la Información Personal; (vii) Medidas de Seguridad; (viii) Acceso y Corrección; y, (ix) Responsabilidad. Cítese los principios contenidos en: (i) Convenio 108 de 1981 del Consejo de Europa del 28 de enero de 1981; (ii) Resolución 45/95 del 14 de diciembre de 1990 de la Asamblea General de la ONU; y, (iii) Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal.

40 "ARTÍCULO 4o. PRINCIPIOS DE LA ADMINISTRACIÓN DE DATOS. En el desarrollo, interpretación y aplicación de la presente ley, se tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen: a) Principio de veracidad o calidad de los registros o datos; b) Principio de finalidad; c) Principio de circulación restringida; d) Principio de temporalidad de la información; e) Principio de interpretación integral de derechos constitucionales; f) Principio de seguridad; y, g) Principio de confidencialidad".

41 "Artículo 4°. Principios para el tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios: a) Principio de legalidad en materia de tratamiento de datos; b) Principio de finalidad; c) Principio de libertad; d) Principio de veracidad o calidad; e) Principio de transparencia; f) Principio de acceso y circulación restringida; g) Principio de seguridad; h) Principio de confidencialidad". Véase también: (1) principio de necesidad (2) principio de utilidad; (3) principio de integridad en el manejo de datos; (4) principio de incorporación; (5) principio de individualidad, citados en la sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

da, entendida y aplicada en todo el grupo empresarial, y tengan un comportamiento diligente en todas las actividades que tengan relación con el manejo de información.

El principio de finalidad consiste en que el tratamiento de datos debe obedecer a un objetivo específico, legítimo y que debe ser puesto en conocimiento del titular de la información. En ese sentido, la Corte Constitucional, en Sentencia C-1011 de 2008, M.P. Jaime Córdoba Triviño, indicó que: "[queda] prohibida (i) la recopilación de información personal sin que se establezca el objetivo de su incorporación a la base de datos; y (ii) la recolección, procesamiento y divulgación de información personal para un propósito diferente al inicialmente previsto y autorizado por el titular del dato". Por tanto no está autorizada la transferencia de datos para finalidades distintas a los que previamente ha consentido el titular (Gozaíno, 2001, p.198).

En cuanto al principio de libertad, el legislador estatutario dispuso que el tratamiento de un dato solo pueda ejercerse con el consentimiento previo, expreso e informado del titular de datos, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos de manera ilícita[42]. Adicional a lo anterior, en la Sentencia C-748 de 2011[43], dijo la Corte que: "no **está permitido el consentimiento tácito del Titular del dato**".

El principio de transparencia, también denominado de publicidad del tratamiento, obliga a que la información, en lo que respecta a la recolección, administración y transferencia de datos, debe ser comunicada cuando lo requiera el titular de datos.

Como lo señaló Gabriel Freixas Gutiérrez (2001, p. 166) "[el principio de transparencia] intenta dar el máximo conocimiento a los ciudadanos, afectados o no, de la existencia de ficheros en los que consten datos de carácter personal". En síntesis, transparencia significa, entre otros, no realizar tratamiento de datos ocultos o secretos.

El principio de acceso y circulación restringida está destinado a garantizar que el tratamiento de los datos solo podrá hacerse por personas autorizadas por el titular[44]. Asimismo, la Corte Constitucional, en la Sentencia C-1011 de 2008[45], señaló que: "el derecho que tiene el sujeto concernido de acceder a su información personal tiene carácter inalienable". Por tanto, el acceso a la información garantiza al titular el conocimiento de la recolección de sus datos personales y el tratamiento al que están siendo sometidos.

Por otra parte, el principio de seguridad de los registros (literal f del artículo 4º), tiene como ob-

42 Véase las sentencias T-022 de 1993, SU-082 de 1995 M.P. Jorge Arango Mejía, T- 580 de 1995 M.P. Eduardo Cifuentes Muñoz, T- 552 de 1997, T-527 de 2000, T-729 de 2002, T-727 de 2007, T-657 de 2005 M.P. Clara Inés Vargas Hernández, y T-684 de 2006 M.P. Marco Gerardo Monroy Cabra. T-658 de 2011 M.P. Jorge Ignacio Pretelt Chaljub.

43 M.P. Jorge Ignacio Pretelt Chaljub.

44 La Corte Constitucional en Sentencia T-729 de 2002, M.P. Eduardo Montealegre Lynett, indicó que: "el principio de circulación restringida, estrechamente ligado al de finalidad, la divulgación y circulación de la información está sometida a los límites específicos determinados por el objeto de la base de datos, por la autorización del titular y por el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales". Ver Sentencia T-216 de 2004, M.P. Eduardo Montealegre Lynett, y Resolución 25914 del 21 de mayo de 2010, Superintendencia de Industria y Comercio (SIC). .

45 M.P. Jaime Córdoba Triviño.

jetivo evitar la adulteración, pérdida, consulta, acceso no autorizado o fraudulento de los datos del sujeto. Por ello, la seguridad en los bancos de datos son una garantía de la integridad, disponibilidad y de la protección de la información.

Para concluir este título, es preciso decir que la Corte Constitucional, en la Sentencia C-748 de 2011[46], incorporó otros principios a los enunciados en el artículo 4 de la Ley 1581 de 2012. En efecto, indicó el Alto Tribunal que existen unas reglas rectoras en el proceso de administración de datos personales derivadas directamente de la Carta Política, específicamente: (i) la prohibición de discriminación por las informaciones recaudas en las bases de datos; (ii) el principio de interpretación integral de los derechos constitucionales; y, (iii) la obligación de indemnizar los perjuicios causados por las posibles fallas en el proceso de administración de datos. Señaló, además, que concurren unos principios originados del núcleo temático del proyecto de ley estatutaria, a saber: (i) principio de la proporcionalidad del establecimiento de excepciones; (ii) principio de autoridad independiente; y, sobre todo para efectos del presente trabajo, el (iii) principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos. Sobre este último principio, recalcó la Corte Constitucional que: "existe una prohibición de transferencia internacional a cualquier tipo de países que no proporcionen niveles adecuados de protección de datos".

Así las cosas, los principios relativos a la protección de datos de personas se constituyen como una herramienta para verificar la protección y efectividad de los derechos involucrados en el tratamiento de datos personales a través de las NCV.

2. Sistemas de auditorías

Un sistema de auditoría es un "procedimiento encaminado al control y supervisión que permite descubrir fallos en las estructuras o vulnerabilidades existentes en la organización de una empresa en materia de Protección de Datos de Carácter Personal" (LOPDatos Consultores).

En este sentido, se observa que a juicio del Informe de Trabajo Número 74, la auditoría puede ser interna, externa o mixta, prestada por personas acreditadas ante las agencias de protección de datos de la Unión Europea. Asimismo, en el Documento de Trabajo Número 108, se establece que este mecanismo incluye el control de todos los aspectos de las NCV, incluido el seguimiento de las medidas coercitivas por violación a las normas vinculantes y protección de datos.

El Informe Número 153 indica que en la solicitud presentada ante las autoridades de protección de datos se debe contener una descripción detallada del sistema de auditoría que se pretende adoptar. El numeral 2.3 señala que el grupo corporativo solicitante debe acreditar: (i) el programa de auditoría a emplear; (ii) la entidad encargada de auditar; (iii) la periodicidad de la evaluación; (iv) la cobertura de la auditoría; y, (v) los informes que deben presentar.

Igualmente, en el Documento Número 154, el Grupo de Trabajo insiste en que el grupo multi-

46 M.P. Jorge Ignacio Pretelt Chaljub.

nacional garantice que cada miembro del grupo acepte la implementación de sistemas de control[47].

Hay que señalar que el sistema de auditoría evalúa la coordinación que existe entre las diferentes sociedades del mismo grupo empresarial (Chen, 2008, p. 226). El derecho a la protección de los datos supone la existencia de un personal adecuado e independiente que gestiona, supervisa y valora periódicamente la eficacia de la política de privacidad, etc.[48]

3. Descripción del procedimiento y los flujos de información

En el Documento de Trabajo Número 74, el Grupo de trabajo asume que las NCV deben contener un nivel razonable de detalle en la descripción de los datos, procesamiento y finalidad del tratamiento; hace hincapié en que el grado de detalle debe ser suficiente para que una autoridad de datos pueda constatar si la transferencia de datos es adecuada.

Por otro lado, en concordancia con lo dispuesto en el Informe de Trabajo Número 74, los informes números 107 y 108 disponen que en las normas corporativas se deben identificar la naturaleza y la estructura de la operación. El Informe Número 108 señala que el grupo debe acreditar si en las NCV se refieren a un solo tipo de datos o a un conjunto de datos. Asimismo, debe indicar cuál es la finalidad de la transferencia de la información.

El Documento de Trabajo Número 133 reitera que el solicitante debe proporcionar una breve descripción del alcance y la naturaleza de los datos. El Informe Número 154 señala que el grupo empresarial debe acreditar cuál es el alcance de aplicación de las NCV en los diferentes miembros del grupo, el ámbito geográfico donde se va a desarrollar el procesamiento de los datos (automático o manual), y la aplicación material de la transferencia, naturaleza de los datos (clientes, empleados o proveedores). Se reitera en dicho escrito que el grupo corporativo debe acreditar ante las autoridades de protección de datos, la naturaleza de la información, la finalidad de la transferencia y los que ostentan la calidad de importadores y exportadores de datos.

4. Instrumentos de reclamos y quejas

Como lo ha señalado Miralles (2010, p. 22), las NCV deben ser vinculantes también para el beneficio de las personas. Se está hablando, por tanto, de un derecho en cabeza de los titulares de iniciar las reclamaciones en caso de una manipulación ilegal de sus datos, información inexacta, incompleta y no veraz, o ausencia del consentimiento previo del titular.

Se tiene que en el Informe de Trabajo Número 74, se establece que los interesados incluidos

47 "La confianza en el respeto de tales principios, una vez efectuada la transferencia, mejoraría si el cumplimiento de los mismos por parte del receptor quedase sujeto a una verificación externa, de la que podría encargarse, por ejemplo, una empresa de auditoría especializada o un organismo de normalización o certificación" (Grupo de Trabajo del Artículo 29, 1998).

48 "La realización periódica de auditorías transparentes por parte de sujetos cualificados y preferentemente independientes, que verifiquen el cumplimiento de la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, así como de los procedimientos establecidos por la organización a tal efecto". Literal d, del estándar internacional No. 22 de la Resolución de Madrid.

en el alcance de las NCV, tienen derecho a exigir el cumplimiento de las normas mediante un sistema de quejas, peticiones o reclamos. Por tanto, se requiere de la creación de una oficina independiente al resto del grupo empresarial, en el ejercicio de sus funciones. Por su parte, el Documento de Trabajo Número 154 contempla que mediante los mecanismos internos de quejas y reclamos, el titular podrá informar de cualquier miembro del grupo que no esté cumpliendo con las políticas corporativas.

Asimismo, en el Informe Número 153 se reitera la necesidad de que las NCV deben contemplar cuáles son los derechos que gozan los titulares de los datos como terceros beneficiarios para hacer cumplir las normas. Además, vale la pena destacar, de acuerdo con las apreciaciones de Carnikian (2010, p. 27), que el grupo debe informar al interesado beneficiario cuál es la oficina donde puede ejercer sus derechos o realizar alguna denuncia en el tratamiento de sus datos.

En este punto también debe tenerse en cuenta que la Resolución de Madrid insiste en que la persona responsable de los datos deberá implementar procedimientos que permitan a los interesados ejercer sus derechos de forma sencilla, ágil y eficaz, y que no conlleven demoras o costes indebidos, ni ingreso alguno para la persona responsable (Numeral 2, del estándar internacional No. 19).

Se puede afirmar que el sistema de PQRs es un "medio imprescindible"[49] para la efectividad, exigibilidad y protección de los derechos de las personas en el tratamiento de sus datos. Este mecanismo, es sin lugar a dudas, la mejor herramienta con que cuentan los titulares de los datos para evaluar si las NCV, son una verdadera política corporativa, para saber con exactitud donde se encuentran sus datos, el tratamiento del que están siendo objeto, solicitar la actualización, rectificación, complementación o retiro de la información de los ficheros de datos, en caso negativo, el grupo debe tomar las medidas necesarias en caso que se incumpla lo previsto en ellas.

5. Responsabilidad

El Informe Número 74 contempla que el grupo multinacional debe remediar los actos en que han incurrido los miembros de su organización, y, en su caso, responder pecuniariamente por el incumplimiento de lo contemplado en la política corporativa.

Por otro lado, el Informe de Trabajo Número 108 establece que la carga de la prueba, respecto a una supuesta infracción de las NCV, le corresponde al miembro del grupo que originó la transferencia de la información, independientemente de dónde se originó el reclamo.

Así, en el Informe de Trabajo Número 154 reitera lo dicho en el informe de Trabajo Número 74, en el cual establece que es necesario que el grupo corporativo garantice al momento de solicitar la aprobación de las Normas Corporativas Vinculantes que cuenta con activos suficientes para asumir la carga indemnizatoria para resarcir los daños y perjuicios que se puedan producir del incumplimiento de las NCV.

49 Sentencia C-1011 de 2008. M.P. Jaime Córdoba Triviño.

De otra parte, el Grupo de Trabajo insiste en que los titulares de información deben ser capaces de instaurar las respectivas reclamaciones por las violaciones de sus derechos ante las autoridades judiciales.

En cuanto a la exoneración de la responsabilidad por cualquier violación de las NCV, la propuesta de reforma de la Directiva 95/46/CE establece explícitamente que: "el responsable o el encargado del tratamiento sólo podrán ser exonerados de esta responsabilidad, total o parcialmente, si prueban que el acto que originó el daño no es imputable a dicho miembro" (literal f, del numeral 2, artículo 43).

Se observa también que la Resolución de Madrid dispone que: "La persona responsable será responsable de aquellos daños y/o perjuicios, tanto morales como materiales, que hubiesen causado a los interesados como consecuencia de un tratamiento de datos de carácter personal que hubiese vulnerado la legislación aplicable en materia protección de datos, a menos que pueda demostrar que el daño no le puede ser atribuido" (estándar internacional No. 25).

A simple vista, se trata de una obligación que recae sobre el responsable de la trasferencia con el fin de garantizar y demostrar que cada operación de tratamiento cumple lo dispuesto en sus normas grupales.

Otros elementos que deben estar contenidos en el programa de las NCV, de manera resumida, son los siguientes:

- **Transparencia y publicidad frente al tercero:** se ha planteado en el Informe de Trabajo Número 74 la necesidad de que los interesados tengan conocimiento previo de que sus datos van a ser transferidos y procesados fuera del territorio. Sin embargo, reitera la necesidad en que el solicitante facilite y permita el libre acceso de la información a los interesados con el fin de que verifiquen el cumplimiento de las normas por parte del mismo grupo. Por ejemplo, en el Informe Número 154, se indica que el grupo puede publicar en la página web de la empresa el contenido de las NCV para conocimiento del personal y terceros beneficiarios. Lo anterior obedece al derecho que tienen los individuales de tener el control de sus datos personales.

- **Colaboración con las autoridades de control y vigilancia:** la colaboración entre el grupo corporativo con las autoridades de protección de datos es de vital importancia. Al respecto debe destacarse que, según el informe número 74, las autoridades recibirán una copia del resultado de las auditorías realizadas en la multinacional; esto facilita la tarea de las autoridades de protección de datos de velar por el cumplimiento de la legislación y por los derechos de las personas.

- **Delegado de protección de datos:** para garantizar una protección integral en la circulación libre de datos de carácter personal, la propuesta de reforma de la Directiva 95/46/CE adopta la figura de delegado de protección de datos. El literal b, del numeral 1 del artículo 37 contempla que es una función del delegado la de "supervisar la implementación y aplicación de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la

formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes". Nótese además que literal h, del numeral 2 del artículo 43 de la Propuesta de Reforma de la Directiva 95/46/CE, contempla que es obligación del delegado de protección de datos la de supervisar el cumplimiento de las NCV, así como la supervisión de la formación y de la tramitación de las reclamaciones.

- **Actualización:** el Informe de Trabajo Número 74 dedica una parte del escrito a las condiciones que debe acreditar el grupo para que pueda actualizar las normas que afectan de manera significativa la protección de datos, sin que se requiera una nueva autorización de las NCV. El Grupo de Trabajo dispone que se deben cumplir tres condiciones: (i) el miembro responsable debe acreditar que el nuevo participante esté vinculado efectivamente a lo dispuesto en las normas; (ii) se requiere actualizar la lista de miembros y registrar los cambios efectuados a las reglas; y (iii) remitir un informe a las autoridades de protección de datos en el cual se reporte y justifiquen las actualizaciones a las normas o cambios de la lista de los miembros.

6. Autorización

El Informe de Trabajo número 74 señala que el estudio que realizan las autoridades de protección de datos al momento de evaluar las NCV, consiste en efectuar un análisis de las garantías adoptadas por los solicitantes, con el fin de verificar si proporcionan una protección adecuada de los datos.

Se tiene además que la autoridad debe conocer cuál es la estructura básica del grupo. Por ejemplo, en el Documento de Trabajo Número 107, el Grupo de Trabajo obliga al solicitante, en el momento en que se postula, a informarle a la autoridad de las actividades económicas y lugares donde se encuentran ubicadas las filiales a las que se van a trasferir los datos. A ello se suma que, en el Informe de Trabajo Número 108 reproduciendo lo dispuesto en los informes No. 74 y 107, se reitera en que el peticionario debe acreditar cuál es el miembro del grupo, dónde se toman las decisiones, los medios y fines del tratamiento. Asimismo, el Grupo de Trabajo en los diferentes informes de trabajo insiste en la necesidad del conocimiento acerca de la cantidad de datos que está procesando el grupo empresarial que deben tener las autoridades de protección de datos.

En ese mismo sentido, al revisar la constitucionalidad de las NCV, la Corte Constitucional consideró que "para que estas normas cumplan su objetivo, una vez el Gobierno Nacional las reglamente y las organizaciones las implementen, **deben ser revisadas por la autoridad de protección,** función que no fue enlistada en las funciones que se le van a asignar al mencionado ente"[50].

En otras palabras, como lo presenta Barceló & Pérez (2008, p. 157) al momento de otorgar la autorización, las autoridades de protección de datos deben verificar que el solicitante aporte las garantías necesarias de respeto de la protección de los datos de los titulares, sus dere-

50 Negrillas fuera del texto original. Sentencia C-748 de 2011 M.P. Jorge Ignacio Pretelt Chaljub.

chos y libertades fundamentales y se garantice el ejercicio efectivo de sus derechos.

En el capítulo II de este documento se esbozó una panorámica general de la estructura orgánica de las NCV, como un sistema de "autorregulación" que ofrece las garantías suficientes para la trasferencia de datos personales a destinos que no garanticen un nivel equiparable de seguridad en la protección de la información, materializado en una verdadera política mundial. Un elemento central de este enfoque es su carácter vinculante y obligatorio para todo el grupo empresarial (exigibilidad jurídica interna y externa). Otro punto importante es que la implementación de las normas corporativas está supeditada a que las autoridades de protección de datos emitan su autorización. Finalmente, no hay que olvidar que la Unión Europea no concibe la "autorregulación", como una herramienta que reemplace el marco legal.

Al margen de utilizar las normas corporativas para ofrecer las garantías adecuadas, la doctrina ha trabajado sobre la posibilidad de que los grupos empresariales utilicen "sellos de certificación" como un sistema que acredita el nivel de cumplimiento de la ley en el tratamiento de los datos personales, como veremos en el siguiente capítulo.

III. SISTEMAS DE ACREDITACIÓN EN EL CUMPLIMIENTO DE LAS NORMAS DE PROTECCIÓN DE DATOS: SELLOS DE CERTIFICACIÓN

En el Informe de Trabajo Número 173, el Grupo de Trabajo del Artículo 29 recalcó el alcance del principio de responsabilidad en el tratamiento de datos y la necesidad de reforzar su estructura interna mediante la adopción unilateral de estrategias y procedimientos que superen los requisitos mínimos establecidos en las normas y reglamentos de protección de datos, por parte de los responsables del proceso.

En el documento se hace hincapié en que las autoridades se deben mostrar confiadas en que los responsables de datos, con el fin de mantener una buena reputación y ganar la confianza de los terceros beneficiarios, acepten adoptar medidas adecuadas y suficientes de protección de datos, orientados a disminuir los riesgos jurídicos, económicos y de prestigio que se puedan generar en la actividad, y lograr una menor probabilidad de una violación a la normatividad por parte del responsable.

El Grupo de Trabajo (2010, p. 19) aborda por primera vez el concepto de "programas" o "sellos de certificación". Señala que mediante esta herramienta el grupo corporativo solicitante podrá demostrar ante las autoridades de protección de datos que ha adoptado medidas concretas, adecuadas y eficaces en la transferencia internacional de datos. Indica el informe que: "una autoridad de protección de datos sólo podría usar la certificación expedida por un programa

de certificación dado, al analizar con arreglo a las [NCV], un responsable del tratamiento de datos ha aportado garantías suficientes al objeto de transferencias internacionales de datos, contribuyendo así a racionalizar el proceso de autorización de transferencias internacionales de datos". Igualmente, el artículo 39, numeral 1 de la propuesta de reforma de la Directiva 95/46/CE trae a colación la creación de mecanismos de certificación en materia de protección de datos, como una herramienta por la cual los interesados podrán evaluar rápidamente el nivel de protección que ofrecen los responsables y los encargados de datos.

Adicionalmente, cabe mencionar que Antonio Troncoso Reigada (2010, pp. 244-250) recalca que la misma industria ha desarrollado sus propios estándares internacionales sobre privacidad y protección de datos por encima de los contemplados en la normativad existente, movidos por un legítimo interés de comercializar productos y servicios que solo puede impulsarse a nivel global, mediante la adopción de políticas que garanticen una efectiva y uniforme protección al derecho de la privacidad. Para el citado autor, un elemento que puede contribuir a alcanzar un estándar internacional en lo que se refiere a un mayor grado de protección de los datos de catacter personal, es el establemiento de un modelo de certificación. En cuanto a las ventajas, el autor señala que:

"El establecimiento de un sello europeo de privacidad para productos y servicios de tecnologías de la información en los sectores público y privado es positivo para los consumidores porque proporciona criterios objetivos para determinar si un producto o servicio es respetuoso con el derecho fundamental a la protección de datos personales" (Reigada, 2010, p. 252).

Es así como el espíritu de los programas de certificación es garantizar una verdadera política de protección de datos de carácter personal, y esto se manifiesta en la preservación de la confianza frente a los titulares de los datos.

En todo caso, cabe resaltar que el que una empresa disponga de un sello de certificación no garantiza que no se infrinjan las normas de protección de datos. Esto implica que el otorgamiento de un sello de certificación no supone la aprobación de sus NCV, sino, por el contrario, es una herramienta que permite a las organizaciones multinacionales reforzar sus políticas internas y evaluar el nivel de protección de sus normas corporativas.

Se debe aclarar, además, que las autoridades de protección de datos no son entidades de certificación. Para Troncoso Reigada (2010, p. 256) "es importante no confundir los reguladores con los regulados: la autoridad de control son las Agencias de Protección de Datos; la autoridad de certificación y las empresas de auditoría son sectores regulados y sometidos a control". De tal forma que para el citado autor, el papel de las autoridades es la de supervisar la buena calidad de los programas de certificación y "velar por el cumplimiento de la legislación de protección de datos y de controlar su aplicación".

De este rápido panorama se puede concluir que debe existir una auténtica política de publicidad y transparencia en la definición de criterios, re-

glas y procedimientos que doten de un juicio de objetividad e independencia a la autoridad de certificación.

No obstante, hay quienes como Eric Lachaud (s.f.), proponen que este programa sea considerado como un mecanismo alternativo para efectuar transferencias internacionales de datos personales a países que no cuenten con un nivel adecuado de protección, sin necesidad de que se celebren cláusulas contractuales tipo o se adopten las NCV.

En esa dirección sostiene que el sistema de certificación es más económico y accesible para las pequeñas y medianas empresas que las NCV, dada su complejidad y costo al momento de implementarlas en la estructura organizativa.

Referente al sistema de costos, Blas (2009, p. 58) afirma que "el sistema de [NCV] es probablemente, por lo menos a nivel intracorporativo, el instrumento más avanzado en materia de transferencia y política global de privacidad. Sin embargo, queda mucho por desarrollar ya que viendo los costes necesarios y la complejidad y variedad de los criterios para tener aprobadas las [NCV] en 30 países, es un ejercicio extremadamente lento y costoso. El elevado costo de las [NCV] al requerir a la compañía documentar sus procesos de tratamiento de datos a la satisfacción de cada autoridad nacional reguladora de protección de los datos en cada jurisdicción en la cual funcione en Europa es capaz de desanimar a las empresas más grandes y modernas".

Los sellos de certificación permiten a las autoridades garantizar que la transferencia internacional de datos sea compatible con las libertades y derechos fundamentales de las personas (seguridad jurídica), a través de auditorías periódicas. El sistema admite un monitoreo constante con el fin de verificar que las obligaciones suscritas con las entidades de certificación se cumplan en la práctica (Lachaud, s.f. pp. 1-5).

En otras palabras, lo que busca el profesor Lachaud es incentivar el uso de programas de certificación mediante los cuales se garantice el cumplimiento de los principios de protección de datos. Este argumento ha sido desarrollado en la legislación mexicana.

A. Primeros pasos en el caso Mexicano

Uno de los puntos centrales de la regulación del tratamiento de datos de carácter personal que tuvo finalmente el desarrollo en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, es el reconocimiento de la transferencia nacional o internacional de datos sin el consentimiento del titular cuando sea efectuada a sociedades controladas, subsidiarios o afiliadas bajo el control común del responsable, o cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas (fracción III, del artículo 37).

El reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares recoge esta habilitación en su artículo 70, en el cual permite la transferencia dentro del mismo grupo del responsable. Dicho artículo establece que será posible "[la] transferencia de datos personales entre sociedades contro-

ladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, el presente Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando estas cumplan con lo establecido en la ley, el presente reglamento y demás normativa aplicable".

Además, vale la pena destacar que los mecanismos de autorregulación se encuentran reglamentados dentro de la legislación mexicana en el artículo 79, el cual dispone que "las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos personales, que complementen lo dispuesto por la Ley, el presente Reglamento y las disposiciones que se emitan por las dependencias en desarrollo del mismo y en el ámbito de sus atribuciones. Así mismo, a través de dichos esquemas el responsable podrá demostrar ante el Instituto el cumplimiento de las obligaciones previstas en dicha normativa".

En el mismo dispositivo reglamentario se establece que los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos dirigidos a fomentar la protección del derecho a la protección de datos de carácter personal y cumplimiento de la normatividad respectiva (artículo 80).

Dentro de los beneficios de la autorregulación se destaca: "cuando un responsable adopte y cumpla un esquema de autorregulación, dicha circunstancia será tomada en consideración para determinar la atenuación de la sanción que corresponda" (artículo 81).

Paralelamente con lo anterior, el artículo 83 señala que los esquemas de autorregulación vinculantes podrán incluir la certificación de los responsables en materia de protección de datos personales. En cuanto a las calidades de las entidades de certificación, el artículo 84 indica que las personas acreditadas como certificadores tendrán la función principal de, valga la redundancia, certificar que las políticas, programas y procedimientos de privacidad instrumentados por los responsables que de manera voluntaria se sometan a su actuación, aseguren el debido tratamiento y que las medidas de seguridad adoptadas son las adecuadas para su protección. A su vez, en el mismo artículo se hace hincapié en que las personas que sean acreditadas como certificadores deberán garantizar la independencia e imparcialidad para el otorgamiento de certificados.

Conviene mencionar que el modelo mexicano reconoce los beneficios de un sistema de autorregulación que implica un esquema efectivo y transparente que garantice un debido tratamiento de los datos personales. Asimismo, se tiene que el sistema es compatible con otros esquemas que permiten la transferencia internacional de datos como las NCV.

IV. CONCLUSIONES

A lo largo de este trabajo se hizo hincapié en el desarrollo de una nueva herramienta que permite definir un marco de actuación aplicable a las operaciones internacionales en el tratamiento de datos, en el seno de grupos multinacionales. Así, por un lado se observa que se procura garantizar un nivel adecuado de protección a la vida privada y el respeto al derecho fundamental del hábeas data de los ciudadanos siempre y cuando se cumplan unos requisitos. Por otro lado, se permite fomentar la adopción de estándares de privacidad a una pluralidad de destinos que no cuentan con una normativa sobre protección de datos aplicable, o si la tienen es mínima. Se evidencia la necesidad que los esfuerzos internos de protección tendientes a evitar el tratamiento inadecuado y abusivo de los datos personales no se desvanezcan cuando son objeto de una transferencia internacional. Y, finalmente, se busca flexibilizar y simplificar el marco jurídico en la materia.

Las NCV incentivan a las empresas a desarrollar, de manera voluntaria, sus propios programas de protección transfronteriza de datos a nivel corporativo, reflejando con exactitud la naturaleza de su negocio y la forma como aprovechan la información, por encima de los estándares contemplados en la normatividad existente. Ello contribuye a eliminar la celebración de cláusulas contractuales tipo entre todos los integrantes de la corporación, pues las NCV permiten la libre circulación de datos basado en un único instrumento que ofrece las garantías necesarias de protección, de carácter vinculante y obligatorio, dentro, y fuera del grupo. Así, a través de un sistema integral de datos no solo se aumentan la confianza de los titulares en el tratamiento, transferencia y procesamiento de su información, sino que contribuye a la generación de cultura en la protección de datos en el grupo, dada una formación adecuada del personal.

No obstante para que las NCV efectivamente garanticen los derechos de los titulares deben cumplir ciertos requisitos de contenido y efectividad. Así, por ejemplo, la consagración de los principios básicos de protección de datos; procedimientos más ágiles para la recepción y manejo de quejas o reclamos; conocimiento de la información, y manejo de clientes y empleados; programas de educación y formación del personal; sistemas de auditorías internas, externas o mixtas para la identificación de los riesgos que se puedan generar en el tratamiento de la información; colaboración con las autoridades de vigilancia y control; delegados de protección de datos; y, mecanismos de reparación. Estas herramientas se deberían tener en cuenta por el regulador con ocasión del mandato del artículo 27 de la Ley 1581 de 2012.

En cuanto a los "sellos" o "programas de certificación", se puede concluir que generan un "valor agregado" en el tratamiento de los datos personales, mediante el cual una entidad de carácter independiente e imparcial acredita a un grupo empresarial que cumple con políticas transparentes y que dotan de seguridad jurídica a los flujos internacionales de información. Sin embargo, surge el siguiente interrogante, ¿Cuáles son los requisitos que deben acreditar las empresas que expiden los sellos de certifi-

cación? Una problemática adicional que deberá ser resuelta en un futuro trabajo.

En todo caso, no debe perderse de vista que las NCV y los "sellos de certificación", no reemplazan la regulación y el deber constitucional de las autoridades de garantizar a los ciudadanos el debido tratamiento de sus datos personales. En este sentido, son bienvenidas las NCV y los "sellos de certificación", siempre y cuando, el regulador deje claro los mecanismos para que el Estado garantice el respeto del derecho fundamental de la protección de datos. Es por eso que la autoridad de control de Colombia debe vigilar con especial cuidado a las empresas que utilicen las NCV y a las que van a emitir los "sellos de certificación". A estas últimas debe exigírseles responsabilidad por las fallas que genere la emisión de estos sellos frente a las eventuales lesiones de los derechos de los titulares de los datos personales. Lo anterior es así porque al fin y al cabo las empresas que emitan dichos sellos están cumpliendo una función pública de certificación sobre el nivel de protección de datos al interior de una organización.

Adicionalmente, y para concluir, es preciso señalar que la autoridad de control de Colombia debe ser especialmente cuidadosa cuando lleva a cabo una aprobación de las NCV. A nuestro juicio, el permiso debe fundarse en un control material sobre las mismas, control que se circunscribe a examinar el contenido de las garantías respecto al derecho fundamental de los ciudadanos a la protección de sus datos, ofrecidas por el grupo empresarial, de tal forma que estas se armonicen con las normas constitucionales.

Bibliografía

A. Doctrina

Agencia Española de Protección de Datos. Transferencias Internacionales. Aspectos Prácticos. *Seminario Regional de Protección de Datos.* Montevideo: Agencia Española de Protección de Datos.

Barceló, R., & Pérez Asinari, M. V. (2008). *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPD.* Valencia: tirant lo blanch.

Barrio, F. (2006). ¿Regulación o autorregulación de los derechos del consumidor en internet? Esa es la cuestión. *Revista de Derecho Comunicaciones y Nuevas Tecnologías 2.* pp. 123-136.

Blas, F. (2009). Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales. *Revista Derecho del Estado*, 23. pp.37-52

Carnikian, F. (2010). Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos. *Revista, Montevideo. p. 30*.

Chen Sui, S. (2008). *Déficit y oportunidades de la legislación costarricense sobre comercio electrónico: un aporte desde la perspectiva de la seguridad, la protección de datos y los derechos del consumidor.* Tesis doctoral, San José.

Cruz, F. J. (2010). *Las medidas tendientes al resguardo de los datos ayudan a uniformar las políticas de Privacy by Design(10) (PbD), deno-*

minación que apunta a la protección de la información desde el origen de las operaciones y no sólo cuando éstas puedan constituir un riesgo, promoviendo también la autorregulación. Protección de datos y servicios globales: ¿Regulación o incentivo? Santiago de Chile, Chile: Corporación Expansiva.

Cuatrecasas, G. P. (06 de 05 de 2011). *Autorizaciones elásticas: Binding Corporate Rules. Obligaciones básicas en materia de protección de datos* .

Del Peso Navarro, et ál. (2008). *Nuevo reglamento de protección de datos de carácter personal - medidas de seguridad* (Díaz de Santos ed.). Madrid: Emilio del Peso Navarro, Ed.

Freizas Guitiérrez, G. (2001). *La protección de los datos de carácter personal en el derecho español.* Barcelona: Bosch, S.A.

Gozaíno, O. (2001). *HÁBEAS DATA. Protección de Datos Personales.* (R. y. S.A., Ed.) Buenos Aires: Rubinzal - Culzoni Editores.

Pou, M. A. (2006). *Manual Práctico de Comercio Electrónico.* Madrid: L. LEY, Ed.

Remolina Angarita, N. (2010). Cláusulas Contractuales y Transferencia Internacional de Datos Personales. En J. Oviedo Albán. *Obligaciones y Contratos en el Derecho Contemporáneo.* Bogotá: Biblioteca Jurídica Diké, Universidad de la Sabana.

Remolina Angatita, N. (2010). *¿Tiene colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. Revista Colombiana de Derecho Internacional.* pp. 489-524.

Severa, P. G. (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales.* Granada: Comares.

Troncoso Reigada, A. (2010). *La protección de datos personales. En busca del equilibrio.* Valencia: Tirant lo Blanch.

B. Páginas Web

Aerocolombia. (s.f.). *Aerocolombia: Guia de Colombia para extranjeros*. Recuperado el 13 de abril de 2012, de http://aerocolombia.com/2011/10/01/aerolineas-internacionales-con-destinos-en-colombia/mapa-de-rutas-lufthansa/.

Agencia de Protección de Datos de la Comunidad de Madrid. (29 de mayo de 2008). *datospersonales.org*. Recuperado el 15 de abril de 2012, http://www.madrid.org/cs/Satellite?c=CM_Noticia_FA&cid=1142473521566&idRevistaElegida=1142455919293&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales.

Álvarez Rigaudias, C. (2005). "Las transferencias internacionales de datos personales y el nivel equiparable o adecuado de protección de datos". *Actualidad Jurídica Uría Menéndez/12-2005*. Recuperado el 14 de abril de 2012 de http://www.uria.com/documentos/publicaciones/1467/documento/art1.pdf?id=2064.

Arenas Ramito, M. (s.f.). *datospersonales.org.* Recuperado el 03 de marzo de 2012, de http://www.datospersonales.org/.

Arrieta Cortés, R. (2011). "Autorregulación y protección de datos personales". *Revista "en foco".* Recuperado el 20 de abril de 2012, de http://www.expansiva.cl/media/en_foco/documentos/18052011161447.pdf.

Blanco Antón, M. J. (2012). "Transferencias Internacionales de Datos Aspectos prácticos". Seminario Regional de Protección de Datos de la ciudad de Montevideo, Uruguay. Recuperado el 14 de abril de 2010 de http://www.redipd.org/reuniones/seminario_2010/common/ponencias/TIsMariaJoseBlanco.pdf.

Castro Bonilla, A. (s.f.). "La Universidad Estatal a Distancia (UNED)". *La regulación de Internet: un reto jurídico*. Recuperado el 20 de abril de 2012, de http://www.uned.ac.cr/redti/documentos/regulacion.pdf.

Cerda Silva, A. (2008). "Hacia un modelo integrado de regulación y control en la protección de los datos personales". *Revista de Derecho y Humanidades* No. 13/2008/ 121-130. Recuperado el 20 de abril de 2012 de http://www.revistas.uchile.cl/index.php/RDH/article/viewFile/910/796.

Cerda Silva, A. "Algunas consideraciones sobre los códigos de conducta en la protección de los datos personales". *Revista Chilena de Derecho Informativo* 8. 2006. Recuperado el 20 de abril de 2012, de http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewFile/10785/11032.

Domingo D, M. (s.f.). "Data Privacy México". *Razón Y Palabra*. Recuperado el 23 de abril de 2012, de http://www.razonypalabra.org.mx/anteriores/n49/bienal/Mesa%205/Mauricio%20DOmingo.pdf.

Ebay. (s.f.). ebayprivacycenter. Recuperado el 25 de febrero de 2012, de http://www.ebayprivacycenter.com/sites/default/files/User_Corporate_Rules_eBay_-_Spanish_Translation%20_07dec2010_.pdf.

Lachaud, E. (s.f.). *Certifying compliance of cross-border flows.*Recuperado el 18 de marzo de 2012, de: http://ec.europa.eu/justice/news/consulting_public/0006/contributions/citizens/lachaud_eric_en.pdf.

Lazaro Esquenazi, J. (2011). *Hewlett-Packard Development Company, L.P.* Recuperado el 4 de diciembre de 2011, de Hewlett-Packard Development Company, L.P: http://www.redipd.org/reuniones/seminario_2011_Cartagena/common/Ponencias/JacoboLazaroEsquenaziFranco.pdf.

Legitec. (s.f.). Recuperado el 28 de febrero de 2012, de:http://www.legitec.com/BCR_NCV.html.

LOPDatos Consultores. (s.f.). *Máxima experiencia en protección de datos LOPDatos Consultores.* Recuperado el 05 de agosto de 2012, de: http://www.lopdatos.es/auditoria.php.

Matus Arenas, J. (junio de 2010). *Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos.* Recuperado el 15 de abril de 2012,

de: http://www.redipd.org/reuniones/seminario_2010/common/ponencias/Ponencia_J_Matus.pdf.

Miralles, R. (2010). *Cloud computing y protección de datos.* Recuperado el 28 de noviembre de 2011 de http://idp.uoc.edu

Valverde López, M. (01 de abril de 2009). *"Las reglas corporativas vinculantes (binding corporate rules) en materia de protección de datos".* Recuperado el 18 de febrero de 2012 de http://es.scribd.com/doc/52311596/BINDING-CORPORATE-RULES.

C. Documentos internacionales

Comisión Europea. (2012). *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) .* Propuesta, Comisión Europea.

Instrucción 1/2000, de la Agencia Española de Protección de Datos (AEPD).

Grupo de Trabajo del artículo 29. (1998). *Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE .* Documento de Trabajo, Comisión Europea.

Grupo de Trabajo del artículo 29. (2003). *Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers.* Documento de Trabajo, Comisión Europea.

Grupo de Trabajo del artículo 29. (2005). *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules".* Comisión Europea.

Grupo de Trabajo del artículo 29. (2005). *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules.* Comisión Europea.

Grupo de Trabajo del Artículo 29. (2008). *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules.* Comisión Europea.

Grupo de Trabajo del artículo 29. (2008). *Working Document Setting up a framework for the structure of Binding Corporate Rules .* Comisión Europea.

Grupo de Trabajo del artículo 29. (2009). *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules .* Comisión Europea.

Grupo de Trabajo del artículo 29. (2010). *Dictamen 3/2010 sobre el principio de responsabilidad.* Informe de Trabajo, Comisión Europea.

Grupo de Trabajo Temporal Sobre Autorregulación y Protección de Datos Personales. (2006). Documento, Red Iberoamericana de Protección de Datos, Santa Cruz - Bolivia.

Resolución de Madrid. (2009). *Estándares Internacionales sobre Protección de Datos Personales y Privacidad .* Resolución, Madrid.

TI/000040/2009 (Agencia Española de Protección de Datos 09 de junio de 2009).

WP 154. (2008). *Working Document setting up a framework for the structure of Binding Corporate Rules.* Articule 29 Data Protection Working Party.

III Encuentro Iberoamericano de Protección de Datos. 2004. *Declaración de Cartagena de Indias - Colombia.* Declaración, Red Iberoamericana de Protección de Datos, Cartagena de Indias.

IV Encuentro Iberoamericano de Protección de Datos. (2005). *Declaración de México.* Red Iberoamericana de Protección de Datos, Ciudad de México -Huixquilucan.