RETOS ACTUALES PARA LA PROTECCION DE DATOS PERSONALES EN LAS ORGANIZACIONES

Mag. Abogado María del C. Becerra[1], Mag. Licenciada Mirta Elizabeth Navarro [2]


Universidad Nacional de San Juan, FFCEF y N , Proyecto Código Nº21/E/871

"Convergencia de Tecnologías informáticas y Metodologías para la implementación de sistemas de Información". e-mail: marisabecerra2005@yahool.com.ar, mirthaenavarro@yahoo.com.ar

Abstract: Los datos personales se han convertido en uno de los activos más importantes de las organizaciones empresariales que buscan liderar el Mercado digital. La recolección, agregación y análisis de datos personales de clientes potenciales es a menudo una parte importante de sus actividades económicas, el desafío que se plantea actualmente consiste en ganarse la confianza de los consumidores reacios a comprar en línea y aceptar suevos servicios. El reto de La Unión Europea sobre la reforma integral de las normas comunitarias de protección de datos, se ha convertido en la problemática de los países latinoamericanos, en nuestro país contamos con una legislación que nos permitió posicionarnos entre los países que brindaban una protección adecuada a los datos personales, sin embargo ante la reforma comunitaria la norma vigente debería ser motivo de debate en nuestro país, sostenemos que las empresas necesitan normas modernas y coherentes en todo el mundo para que los datos fluyan libremente de un país a otro, reduciendo la burocracia de su adopción para estimular un crecimiento de la Economía Nacional y alcanzar cierto grado de competitividad con la industria mundial.

[1] Abogado, egresado de la UCC. Magíster en Informática egresado de la Universidad Nacional de la Matanza. Docente Investigadora de la U.N.S.J. Directora del Instituto de informática del Foro de Abogados de San Juan

[2] Licenciada en Administración de empresas egresada de la U.N.S.J. Magíster en Gestión de Organizaciones egresada de la Universidad de Valparaíso. Chile. Docente de la U.N.S.J. Directora del Proyecto Convergencia de Tecnologías informáticas y Metodologías para la implementación de Sistemas de información

Palabras Claves: Transferencia Internacional de Datos. Protección de datos en un mundo globalizado. Normas Corporativas Vinculantes.

I. Introducción:

La preocupación sobre la privacidad, podemos decir que ha alcanzado una escala global, actualmente, desde los Estados de la Unión Europea, hasta la mayoría de los gobiernos latinoamericanos están adoptando mecanismos legales de privacidad y protección de datos en sus legislaciones.

Si bien la mayoría de las Constituciones de los países latinoamericanos garantizan el derecho a la intimidad y la privacidad, explícita o implícitamente en materia de protección de los datos personales carecían hasta hace no poco tiempo de leyes especiales en la materia, y solo podían mencionarse como casos excepcionales Argentina, Chile, Paraguay.

Argentina era considerada en el contexto de las naciones de América Latina, como una de los países que cuentan con la legislación más avanzada en materia de Protección de datos personales, situación que le ha permitido ser calificada por el grupo creador del art. 30 de la Directiva Europea 95/46 como el país que cumple la normativa, sin embargo esta situación podría haber cambiado con la sanción de Leyes más modernas sobre protección de datos en países como Colombia, México y Perú.

En los últimos años varios países han legislado sus normas: Uruguay (2008), México (2010), Colombia (2010), Costa Rica (2011), Perú (2011) y Nicaragua (2012). También se puede mencionar la Red Iberoamericana para la Protección de datos personales integrada por 22 países entre ellos: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay , Venezuela.

En la reunión de la Red realizada en el año 2011 formaron parte de la agenda temas como "El impacto de las trasferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos". Algunas de las soluciones para el futuro que se propusieron estuvieron referidas a regulaciones que obligan a las empresas a adoptar políticas globales (como la Resolución de Madrid), y por parte de las empresas que estas adopten normas corporativas vinculantes como Binding Corporate Rules (BCRs) y reglas tras fronterizas de privacidad de APEC (CBPRs)[3].

[3] Son normas elaboradas por las empresas que establecen sus prácticas en relación con cualquier información personal que pueden obtener de sus clientes.

Este tema siempre ha preocupado a la Unión Europea que actualmente se apresta a una reforma integral de las normas de protección de datos, La Comisión Europea propuso una reforma integral que se dio a conocer en la comunicación que envió al Parlamento Europeo, al Consejo y al Comité económico y Social y al Comité de Regiones. La nueva normativa sustituirá a todas las leyes nacionales anteriores y a la Directiva 95/46 de Protección de Datos de la UE, que ha sido parte importante de la legislación europea sobre privacidad y derechos humanos, y bajo la que se han regido las empresas europeas desde 1995.

El intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros ha experimentado un desarrollo sin precedentes, se habla que el mercado para el análisis de conjuntos de datos está creciendo un 40% en todo el mundo. El acceso a una cierta cantidad de datos personales - y la huella digital que la gente deja tras usar Internet durante un periodo de tiempo - son **elementos decisivos en el modelo de negocio** de empresas como Facebook y otras redes sociales. Sin embargo los estados miembros aplicaron la legislación de manera diferente, dando lugar a divergencias de aplicación, por lo que consideran que una sola ley acabaría con la fragmentación actual y costosos trámites administrativos.

Con ello se unificarán las diferentes normativas nacionales en Europa en material de protección de datos, lo que beneficiará sobre todo al mercado único y la protección efectivo de los derechos y libertades fundamentales de las persona. En el año 2011 la Comisión participo de un diálogo con las Autoridades Nacionales de Protección de datos y con el Supervisor Europeo de Protección de datos para analizar algunas opciones sobre la aplicación más coherente de la normativa.

Esto también se verá reflejado en nuestro país y nos retrotrae de nuevo a las palabras del profesor Brenna, que con su extraordinaria grandilocuencia, cobran de nuevo vigencia al decir que [Nos enfrentamos hoy a la cuestión de definir de una vez, tanto en los países centrales como en los nuestros, cuales límites construimos, ponemos, aceptamos y luego respetamos, al poder de la tecnología para cubrir y proteger el reino de la privacidad garantizada….Ello nos conduce a una mirada hacia adentro de nuestros países, aquellos que no pertenecen tampoco a la Unión Europea y que carecen de un sistema de normas de protección mínimas, además de los recursos que parecen imprescindibles para afrontar las adecuaciones que nacieran de su adopción].

Actualmente se torna imprescindible instalar el debate en nuestro país para que las empresas locales puedan reformar sus medidas de seguridad previniendo y evitando violaciones al notificar las violaciones a la protección de datos tanto a la Autoridad Nacional de Protección de datos como a los propietarios de los mismos.

II.- Transferencia internacional de datos:

Hace 17 años la Directiva 95/46/CE introdujo una legislación armonizada en toda Europa, que hizo posible que la trasmisión de datos en los estados miembros se hiciera con la mayor seguridad. En nuestro país en el año 2000 se dictó la Ley de

Protección de datos personales Nª 25.326 (en adelante, LPDP) donde se reguló la transferencia internacional de datos, en su ARTÍCULO 12 se estableció una prohibición generalizada a la transmisión de datos personales de cualquier tipo con países u organismos internaciones o supranacionales, que no proporcionen niveles de protección adecuados.

Salvo las excepciones receptadas por el propio artículo, pareciera no haber salida alternativa para el caso de que el país no posea una regulación considerada "adecuada". No obstante, en la reglamentación del Decreto 1558-2001 de dicho artículo, se precisaron mejor los términos y se estableció:

La prohibición de transferir datos personales *hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados,* ***no rige cuando el titular de los datos hubiera consentido expresamente la cesión***.
No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en
general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta. Facúltese a la DIRECCION NACIONAL DE PROTECCION DE DATOSPERSONALES a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional. Si llegara a la conclusión de que un Estado u organismo no protege adecuadamente a los datos personales, elevará al PODER EJECUTIVO NACIONAL un proyecto de decreto para emitir tal declaración. El proyecto deberá ser refrendado por los Ministros de Justicia y Derechos Humanos y de Relaciones Exteriores, Comercio Internacional y Culto.
El carácter adecuado del nivel de protección que ofrece un país u organismo internacional 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 de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales.*
Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección *cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación,* ***o del***
Amparo que establezcan las cláusulas contractuales *que prevean la protección de datos personales.*

En la práctica, la DNPDP en Argentina[4], recibe un buen número de solicitudes de aprobación de transferencias internacionales, existiendo incluso un formulario

[4] www.jus.gov.ar/**datos-personales**.aspx/

especial para ello: el **Certificado C.01**. Esta cantidad de pedidos, es también consecuencia de que según ha sostenido la DNPDP en numerosos dictámenes[5], EEUU **no posee un adecuado nivel de protección**, obligando así a que cada empresa que quiera transferir datos hacia Norteamérica (el principal país donde están radicadas las empresas proveedoras) deba cumplimentar con este contrato extra aprobado como requisito.

Según la DNPDP, este contrato debe contener como mínimo:
Identificación del exportador y al/los importador/es de los datos;
Indicar la ubicación de la base de dato;
Definir como ley aplicable al tratamiento de datos del contrato de servicios a la Ley Nº 25.326;
Se precisen la naturaleza de datos personales que se transferirán;
La declaración que el tratamiento de los datos se realizará en un total de acuerdo con los principios y disposiciones de la Ley Nº 25.326;
Indicar la finalidad a la que serán destinados dichos datos, verificando que cumpla con los requisitos del art. 4 de la Ley Nº 25.326;
Precisar las medidas de seguridad a las que se sujetarán la transferencia y el tratamiento de datos personales, verificando que la misma cumpla con las pautas habituales del sector y con la normativa vigente;
El compromiso del importador que los datos recibidos serán tratados en un todo y sin excepciones según las instrucciones del exportador y las disposiciones de la Ley Nº 25.326, aceptando que se le apliquen las facultades de la DNPDP y respetando los derechos de los titulares de los datos conforme Ley Nº 25.326, como ser los derechos de acceso, rectificación, actualización, confidencialidad y supresión;
La declaración del importador manifestando que la legislación local aplicable no le impide cumplir con las obligaciones pactadas;
La obligación de destruir, y en su caso reintegrar al exportador, los datos personales objeto de la transferencia cuando finalice el contrato;
Se respetará la jurisdicción de los Tribunales argentinos por cualquier conflicto vinculado a la protección de los datos personales que afecte al titular del dato;
El compromiso por parte de importador de no divulgar ni transferir los datos personales a terceros con excepción que: 1) se establezca de manera específica en el contrato o se requiera para la prestación de servicios de tratamiento, o 2) la cesión sea requerida por una ley aplicable o autoridad competente, en la medida que no excedan lo necesario en una sociedad democrática, es decir, cuando constituyan una medida necesaria para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o administrativas, o la protección del interesado o de los derechos y libertades de otras personas, en cuyo caso deberán notificar de manera Inmediata y por escrito al exportador para evaluar si dicha transferencia afecta las disposiciones de protecciones de datos personales locales y en consecuencia afecte la continuidad del contrato.

[5] Dictámenes DNPDP Nº: 248/05; 270/06; 008/08; 017/09; 028/09; entre otros.

La transferencia internacional de datos a jurisdicciones que se consideran como de protección no adecuada ha venido siendo un problema para las multinacionales desde que se aprobó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas sobre el tratamiento de datos personales y a la libre circulación de estos datos.

Desde la entrada en vigor de la Directiva 95/46/CE, ya mencionada, las empresas privadas utilizaron diferentes procedimientos para legitimar las transferencias internacionales de datos, entendiendo como tales aquellas transferencias que se efectúan fuera de la UE. De forma enumerativa podemos referirnos, en primer lugar, a la autorización de una transferencia solicitando dicha autorización a la autoridad competente en materia de protección de datos del estado miembro de la UE desde el cual se origina la transferencia. A esta actuación le da cobertura jurídica el Articulo 26(2) de la Directiva 95/46/CE, que prevé la posibilidad de que los estados miembros autoricen la transferencia, o transferencias, de datos personales hacia terceros países que no aseguran un adecuado nivel de protección, donde la organización que desea transferir acredita que dispone de las medidas de seguridad suficientes para protegerlos.

Otro procedimiento habitual es la utilización de contratos específicos, los que han probado su validez de forma reiterada, más aún luego de las decisiones de la Comisión sobre cláusulas contractuales estándar y las indicaciones aportadas en dicha materia por el Grupo de Trabajo del Art. 29 de la Directiva 95/46/CE (en adelante Grupo del Art.29) y de las diferentes autoridades competentes en materia de protección de datos que han llevado a las compañías privadas a hacer un uso continuado de este instrumento. En este sentido, las decisiones de la Comisión sobre cláusulas contractuales estándar permiten a los Estados Miembros verificar si un exportador de datos ofrece o no las suficientes garantías para efectuar la transferencia.

No obstante, en el caso de las multinacionales en las que el flujo de datos se produce entre diferentes interlocutores de forma casi simultánea, ha resultado probado que las cláusulas contractuales sólo permiten cubrir una pequeña parte del proceso, lo cual hace pensar que para esos casos tan complejos, en los que diferentes operadores resultan implicados, es necesario incluir códigos de conducta internos que puedan ser parte del contrato. Estos códigos internos están destinados a asegurar que las corporaciones adopten las garantías suficientes para que el tratamiento de los datos se produzca de la manera jurídicamente correcta.

Conforme prestigiosa doctrina de nuestro país el contrato será adecuado a la normativa de protección de datos personales, cuando la prestación de los Servicios se mantenga **dentro del territorio argentino**. Sin embargo, debe mencionarse que las principales prestadoras de Servicios Cloud Computing están alojadas en el exterior de nuestro país (especialmente en EEUU). Vale recordar un debate existente en la actualidad, relacionado con el elemento que indica que un proveedor este o no en el país. Por un lado, se sostiene que basta con la presencia de servidores en el país, otros en cambio sostienen que es necesario que tanto la empresa (con su domicilio legal)

como los servidores se encuentren dentro del territorio argentino. Personalmente considero que dicha discusión no reviste de mayor importancia, ya que basta con que alguno de los elementos (servidores u oficinas) se encuentre en el exterior del territorio para que sean exigibles los requisitos de transferencia internacional.

III. Protección de datos en un mundo globalizado.

En el mundo globalizado de hoy, los datos personales se transfieren desde un número cada vez mayor de fronteras virtuales y geográficas y se almacenan en los servidores de varios países. Cada vez más empresas están ofreciendo servicios de cloud computing, que permiten a los clientes acceder, almacenar datos en servidores remotos. Estos factores exigen una mejora en los mecanismos actuales para la transferencia de datos a terceros países, esto incluye la adecuación de decisiones y la certificación de las decisiones, es decir normas de protección de datos en terceros países y las garantías adecuadas, tales como las clausulas contractuales o normas empresariales vinculantes, a fin de asegurar un alto nivel de protección de datos en las operaciones de tratamiento internaciones y facilitar los flujos de datos a través de las fronteras.

La Comisión Europea propuso nuevas normas sobre la privacidad de los datos en Internet, ella considera que el actual y desafiante entorno digital carece de la eficiencia necesaria para garantizar el derecho a la protección de datos personales, por ello se decide asignar mayor responsabilidad a las compañías para proteger la información de los usuarios. El organismo dijo además que los que quebranten la normativa podrían ser multados con hasta un 2% de su facturación anual. Tras dos años de estudiar los cambios en el uso de Internet y el comportamiento de los consumidores, la Comisaria Europea a cargo de la privacidad de datos, Viviane Reding, dijo estar decidida a darles a las personas un mayor control sobre su información personal. "La protección de datos personales es un derecho fundamental para todos los europeos, pero los ciudadanos no siempre sienten tener el control total de sus datos personales", afirmó Reding, comisaria de Justicia, Derechos Fundamentales y Ciudadanía de la Unión Europea[6]

El marco legislativo de la protección de datos de carácter personal ha causado importantes quebraderos de cabeza a las empresas privadas,- principalmente multinacionales con representación en diferentes países dentro y fuera de la Unión Europea,- para encontrar soluciones innovadoras que pudieran conjugar el correcto cumplimiento de la normativa en materia de protección de datos con sus necesidades comerciales dentro de un marco competitivo. Esta situación se complica aún más si tenemos en cuenta que la armonización de la normativa surgida a raíz de la Directiva Europea ha creado diferentes regímenes dentro de la UE, lo cual dificulta la creación de una solución común para todos los estados miembros. A ello hay que añadir que

[6] http://tn.com.ar/personajes/viviane-reding

una gran parte de los países no pertenecientes a la Unión Europea todavía no disponen de una normativa propia en materia de protección de datos.

La reforma de las normas de la UE de protección de datos asegurara los derechos de las personas sigan manteniéndose cuando los datos personales se transfieran desde la UE a terceros países, y siempre que los datos de las personas sean utilizados o analizados por terceros proveedores de servicios. Esto significara que las normas comunitarias de protección se aplicarán independientemente de la ubicación geográfica de una sociedad.

La protección de datos y las garantías se establecerán en un reglamento de la UE con aplicación directa en toda la Unión o de su planta de procesamiento. Se simplificara el marco regulador por la drástica reducción de la burocracia y la eliminación de formales tales como los requisitos generales de notificación. Solo la autoridad de protección de datos, donde la compañía tiene su sede central será responsable de decidir si la empresa está actuando dentro de la Ley. Se establecerá una coordinación rápida y eficaz entre las autoridades nacionales de protección de datos –ya que el servicio está dirigido a personas en varios Estados miembros – ayudara a asegurar que las nuevas normas de la UE de protección de datos se apliquen con coherencia en todos los Estados miembros. Las autoridades nacionales deben ser reforzadas y ello será necesario para garantizar la aplicación coherente y en última instancia, la aplicación uniforme de las Normas en la UE.

Por ello, y ante las restricciones para las transferencias internacionales de datos establecidas por la Directiva 95/46/CE, donde se establece que "Los Estados miembros deben prever que la transferencia a un tercer país de datos personales únicamente pueda efectuarse cuando el tercer país de que se trate garantice un nivel de protección adecuado y cuando con anterioridad a la transferencia se respeten las disposiciones legales de los Estados miembros adoptadas con arreglo a las demás disposiciones de dicha Directiva".

Finalmente cabe mencionar que con el Acuerdo de Puerto Seguro, aprobado por parte de la Unión Europea, se logro que las empresas de los EEUU que se adhieran al mismo (sólo éstas y no sus filiales en otros países), contarán con la "presunción de adecuación" al nivel de adecuación exigido por la Directiva", según lo establece la propia Agencia Española de Protección de Datos.

De esta manera, grandes potencias como Google o Amazon, están suscriptas al convenio, gozando de esta presunción para sus transferencias de datos con la Unión Europea, logrando de esta manera una mayor agilidad en las transacciones, alternativa que lamentablemente no rige para la República Argentina, que sí fue considerada como país con nivel adecuado en materia de Protección de Datos Personales según la Unión Europea y en los términos de la Directiva N° 95/46/CE8.

La citada declaración significa que a Argentina no se le aplican las restricciones para la transferencia de datos personales, permitiendo el libre flujo de los datos personales

desde la Unión Europea. De manera tal que si la empresa proveedora estuviera dentro de la Unión Europea, la transferencia internacional de datos sería lícita desde la Argentina (siempre reuniendo todos los demás requisitos).

IV.-Normas Corporativas Vinculantes:

Una de las soluciones que han aparecido para operar en este escenario tan complejo, son las reglas corporativas vinculantes (binding corporate rules, de ahora en adelante BCR) que consisten en un código de prácticas basado en los estándares europeos de protección de datos, que las organizaciones multinacionales que han decidido aprobarlas e incorporarlas a su funcionamiento, asumen, hacen propio y siguen de forma voluntaria.

Estas reglas se aplican generalmente entre las compañías pertenecientes a un mismo grupo empresarial, independientemente del lugar donde esté la sede o la nacionalidad de los ciudadanos los datos de los cuales se procesan, siempre y cuando el tratamiento de los datos se origine en la Unión Europea (de ahora en adelante UE). El Grupo del Art. 29 señala que hay dos elementos esenciales que deben estar presentes en todos los casos en los que se acude a las BCR para dar cobertura a la transferencia de datos: a) su naturaleza vinculante; y b) su carácter ejecutivo desde el punto de vista jurídico.

No hay que confundir las BCR con los códigos de conducta establecidos en el Artículo 27 de la misma Directiva (códigos tipo), los cuales se diseñan teniendo en cuenta las necesidades de un sector profesional concreto. La similitud del término, no obstante, es la que lleva a hablar de BCR en lugar de "códigos de conducta internos" para evitar así cualquier posible malentendido.

En este escenario, el 3 de junio de 2003, el Grupo del Art. 29 publicó su Documento de Trabajo (WP 74)[7] sobre BCR para transferencias internacionales de datos. El Grupo de trabajo consideró que ya que las reglas eran vinculantes (tanto jurídicamente como en la práctica) e incorporaban los principios esenciales identificados en el Documento de trabajo (WP12) de 24 de julio de 1998, no había motivo para que las autoridades nacionales no autorizaran las transferencias entre compañías pertenecientes al mismo grupo multinacional.

Las bases de las reglas corporativas vinculantes fueron fijadas en junio de 2003 por el documento del Grupo del Artículo 29 (WP 74) sobre transferencias de datos personales a terceros países, en aplicación del artículo 26(2) de la Directiva de protección de datos. En la parte introductoria de estas bases ya se menciona el hecho de que las DPA reciben continuamente solicitudes de transferencias internacionales, que en muchos casos han requerido soluciones contractuales. No obstante, algunas multinacionales estructuradas de forma compleja y con filiales y empresas anexas por

[7] www.scribd.com/doc/52311596

todo el mundo resultarían más beneficiadas si se decidieran a adoptar "códigos de conducta internos para transferencias internacionales" (de la misma manera que adoptan códigos internos para proteger información confidencial, eliminación de la discriminación, implementación de códigos deontológicos, políticas de respeto al medio ambiente, y muchas otras más). En este sentido el Artículo 26 (2) de la Directiva 95/46/EC ofrece a los Estados Miembros un amplio margen de maniobra.

La naturaleza vinculante de las BCR implica que los miembros de la corporación, así como sus empleados, deben comprometerse a cumplirlas estrictamente. En principio, las reglas deben ser adoptadas por el equipo directivo de mayor responsabilidad del grupo, los cuales deben asegurar su cumplimiento por el resto de la organización en bloque.

En Latinoamérica Leyes como las de Colombia las regulan de la siguiente forma Artículo 28. Normas corporativas vinculantes. El Gobierno Nacional expedirá la reglamentación correspondiente sobre Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países. Nuestra Ley 25326 no establece nada al respecto.

Seguidamente, y de forma esquemática, se enumeran aquellos aspectos esenciales que según la normativa europea deben incluirse en las BCR:

a) Principios básicos:

En cuanto a su contenido, hay que decir que, en atención a su carácter autor regulador, es la organización que elige vincularse a él quien debe determinarlo en su totalidad. En otras palabras, no hay un contenido oficial sino que se trata de soluciones ad casum. No obstante, las reglas deben contener unos principios básicos, que son los siguientes:

- Principio de limitación de la finalidad: los datos serán procesados para una finalidad específica y, consiguientemente, utilizados para cumplir la finalidad inicial
- Principio de calidad de los datos y proporcionalidad: los datos deben ser exactos y actualizados, siempre que sea necesario. Los datos deben ser los adecuados, relevantes y no excesivos en relación con la finalidad para la cual van a ser utilizados.
- Principio de transparencia: los ciudadanos deben ser informados sobre la finalidad del tratamiento de los datos así como de la identidad del responsable y cualquier otra información necesaria para asegurar el uso imparcial de los datos.
- Principio de seguridad: el responsable del fichero tomará las medidas técnicas y organizativas necesarias para minimizar al máximo los riesgos que puedan presentarse durante el tratamiento de los datos.

- Los derechos de acceso, rectificación, cancelación y oposición: los ciudadanos tienen derecho a obtener información sobre todos sus datos personales, a rectificarlos cuando no sean correctos, y a que se cancelen cuando han dejado de ser necesarios. En algunos supuestos, también deben tener la posibilidad de oponerse a su tratamiento.
- Restricciones a posteriores transferencias: posteriores transferencias de datos personales sólo pueden ser autorizadas si la entidad a la que se le transfieren también está sujeta a normas que aseguren un adecuado nivel de protección.

Hay que precisar, no obstante, que existen términos similares con diferentes interpretaciones y que el concepto de "grupo corporativo" puede variar de un país a otro y puede corresponder a realidades muy distintas: desde conglomerados más o menos dispersos e independientes, hasta compañías estructuradas jerárquicamente; desde empresas que comparten actividades económicas muy similares, hasta grupos empresariales con actividades muy diversas. Obviamente estas diferencias estructurales y en cuanto a la actividad impactan sobre la aplicación, diseño y alcance de las BCR y son elementos que deben ser tenidos en cuenta por las compañías cuando deciden implementarlas.

Para conglomerados más relajados jerárquicamente, las BCR posiblemente no sean la mejor solución ya que la diversidad de formas y el amplio abanico de actividades y tratamientos pueden hacer muy difícil (sino imposible) su aplicación. Para estos grupos empresariales puede ser más adecuado empezar diferenciando subgrupos dentro de la misma corporación y, partiendo de esa segmentación, particularizar las normas.

En la práctica, las multinacionales son el grupo empresarial más interesado en adoptar BCR para poder regular así las transferencias dentro del grupo y alrededor del mundo. El Grupo del Art. 29 destaca con especial énfasis que las aprobaciones de BCR se limitan a las transferencias o categorías de transferencias dentro del mismo grupo corporativo, es decir, entre empresas obligadas por dichas normas.

b) Información a los interesados

La información mínima que debe darse a los interesados cuyos datos queden sujetos a la aplicación de las BCR debe contener, en un lenguaje comprensible para ellos:

- la finalidad de la transferencia;
- la identificación del exportador de datos establecido en la Comunidad desde el cual se originan los datos personales;
- el receptor de los datos y los países de destino;
- una explicación acerca de que, después de la transferencia, los datos serán procesados por un sujeto no vinculado por las BCR y establecido en un país donde no hay un nivel adecuado de protección de la privacidad . Las auditorias previstas para las BCR deben contener un apartado específico

sobre este tipo de información donde deben constar las revisiones de los contratos de este tipo utilizados por el grupo corporativo. La corporación debe poner a disposición de la DPA y de los interesados el contenido de estos contratos en las condiciones contenidas en las Decisiones de la Comisión antes mencionadas.

V. Procedimiento de Adopción de las BCR

a) Dentro del grupo corporativo:

Podemos resumir el procedimiento de adopción e implementación de las BCR, dentro del grupo corporativo, en los pasos siguientes:

1. En primer lugar, debe aprobarse internamente por la empresa, concretamente por el órgano decisorio más elevado como el consejo de administración o similar, un breve documento (de máximo 3 páginas) destinado a explicar el concepto y el objetivo principal al staff directivo de la organización.
2. Seguidamente, debe crearse un documento genérico que contenga diferentes pasos y reglas, que será distribuido entre la organización. Este documento es el que deberá ser sometido a autorización de la DPA.
3. Deberán crearse también, documentos específicos que contengan normas suplementarias que deban ser utilizadas de forma exclusiva por determinados departamentos (Por ejemplo: recursos humanos, marketing,….)

Tramitación de las BCR ante las DPA:

Los grupos empresariales interesados en conseguir la aprobación de sus BCR deben poder utilizar un procedimiento coordinado entre las diferentes DPA implicadas en el proceso. El principal objetivo es que las empresas puedan utilizar un único procedimiento ante un Estado Miembro que les permita obtener el beneplácito de las diferentes DPA de los Estados Miembros donde el grupo opera.

Descripción de los tratamientos y de los flujos de información.

Las BCR deben identificar los elementos siguientes:

- La naturaleza de los datos, por ejemplo si las BCR se refieren sólo a un tipo de datos (como recursos humanos) o si se refieren a varios tipos. En el supuesto en el que las normas se refieran a varios tipos de datos, deberá indicarse en la solicitud, así como el tipo de garantías establecidas para su protección;
- Las finalidades del tratamiento de dichos datos;

- El número y extensión de las transferencias dentro del grupo cubierto por las BCR. Es necesario incluir detalles sobre: Cualquier miembro del grupo

dentro de la UE desde el que se efectúen las transferencias, Cualquier miembro del grupo fuera de la UE donde se envíen las transferencias.

Tras la reforma introducida por la Comisión Europea este proceso será más sencillo y ágil.

- BCR será validado solo por un DPA, con mecanismos que garanticen la participación rápida de otros DPA pertinentes.
- Una vez que una autoridad ha probado un BCR, será válido para toda la UE sin necesidad de ninguna autorización adicional a nivel nacional.

VI.-Conclusiones:

- La protección de la privacidad en las empresas locales no es la adecuada, hay varias razones que provocan que esta situación delicada, El marco regulador de la protección de datos personales adoptado en nuestro país al igual que el Europeo fue muy estricto en cuanto a la transferencia de datos a terceros países que no contaban con una protección adecuada.
- Actualmente se proyecta una reforma sin precedentes en la Unión Europea en donde las normas corporativas vinculantes se configuran como un instrumento que permitiría a las organizaciones ofrecer garantías para poder llevar a cabo transferencias de datos hacía terceros países, ante ello es necesaria su adopción por parte de las organizaciones locales.
- El marco jurídico debe proporcionar que los elementos se adopten de una manera mejor y más eficaz a los cambios tecnológicos y a la globalización. Además, sería interesante requerir evaluaciones de impacto sobre la privacidad o auditorías regulares para supuestos que entrañen riesgos específicos. Otro punto sería incluir las certificaciones sobre productos o servicios que aseguren una adecuada “privacidad por diseño”.
- Las normas corporativas vinculantes serán una alternativa a las cláusulas contractuales tipo que pueden suscribirse entre exportador e importador de datos para la regulación de una transferencia internacional que suponga un acceso a los datos, cuando el destinatario de estos esté ubicado en un país fuera de la Unión Europea y que no goce de un nivel de protección adecuado. Supondrá además que sean vinculantes porque sean un fiel reflejo de la política de privacidad de la empresa titular de los datos, dándola a conocer públicamente al ciudadano afectado así como al resto de personas físicas y jurídicas que intervienen en el tratamiento, así como en la transferencia.
- En conclusión, la empresa que adopte sus NORMAS CORPORATIVAS VINCULANTES debe estar en condiciones de demostrar que mantiene un férreo control sobre la destinataria de los datos, en tanto y en cuanto esté en condiciones de demostrar que posee y hace cumplir una política de protección de datos “adecuada”, no habiendo razón alguna por la cual no pudiera intercambiar datos personales con otras entidades del mismo grupo establecidas en estados foráneos.

- El mundo de los negocios debe demostrar a las autoridades reguladoras que es capaz de operar de forma global, interactuar a través de redes y aún así respetar la privacidad. No se trata solo de modernizar y endurecer las normas de protección de datos sino de demostrar que la privacidad cuenta y que las empresas deben adoptar voluntariamente las normas corporativas vinculantes y prepararse para colaborar con las autoridades reguladoras para encontrar una solución global a este reto global.
- La protección de datos no es sólo un requisito del negocio de los servicios globales, sino que es un activo agregado del mismo, por lo cual contar con marcos regulatorios adecuados en este ámbito sólo puede generar retornos al país que invierte en ellos, convirtiéndolos en verdaderas plataformas de servicios.

Referencias

1. Brenna, Ramón Gerónimo, Internet y Privacidad. Reflexiones sobre la sociedad de la información y la recolección de datos On Line. Informática y Derecho aportes de Doctrina Internacional. Vol 8. ISBN 950-14 1868-5. Depalma. Buenos Aires.2002.

2. Corrales Marcelo, y otros. El desafío del Cloud Computing dentro del marco legal Europeo .XV Congreso Iberoamericano de Informática y Derecho. Buenos Aires 2011.

3. Molina Quiroga, Eduardo, "Prestigio e imagen del comerciante. Protección de datos personales", en Código de Comercio y normas complementarias. Análisis doctrinario y jurisprudencial, Director Raúl A. Etcheverry, Coordinación: Héctor O. Chomer, Editorial Hammurabi de José Luis de Palma, 2005.

4. Molina Quiroga, Eduardo. Informes crediticios y principio de calidad en el tratamiento de Datos personales. Ponencia presentada en el XV Congreso Iberoamericano de Informática y Derecho. Bs. As. 2011

5. Palazzi, Pablo A., *La transmisión internacional de datos personales y la protección de la privacidad,* Ad-Hoc, Buenos Aires, 2002 La transmisión internacional de datos personales y la protección de la privacidad ISBN: 950-894-318-1

6. Fernández Delpech, Horacio, “Los datos sensibles en la Ley de protección de datos personales. En derecho y nuevas Tecnologías. Año 3. Número Especial. Editorial Ad-Hoc. Noviembre de 2003.-

7. Miguel Sumer Elías, Abogado en Derecho Informático, Buscadores de Contenidos en Internet, Derecho al Olvido y la Decisión de la Justicia (Página consultada el 12 de mayo de 2012).[On-line]. Dirección URL: http://www..forode**abogados**.org.ar/edicion11/tema06.html -

Sitios Web consultados:

http://www.redipd.org/
http://ec.europa.eu/justice/newsroom/data-protection/news/
http:///www.mckinsey.com/mgi/publications/big data

.