EL IMPACTO DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN AMERICA LATINA. LAS POLITICAS PREVENTIVAS Y LA AUTORREGULACION EN LA IMPLANTACION DE LA NORMATIVA DE PROTECCION DE DATOS.

Durante los días 14 al 16 de junio de 2011, se ha celebrado en el Centro de Formación de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), en la ciudad de Cartagena de Indias (Colombia), el Seminario "El impacto de las trasferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de proteccion de datos". En esta ocasión el evento se ha dirigido especialmente a representantes de Instituciones, administraciones y organismos de los países que conforman la Comunidad Iberoamericana, como una de las actividades aprobadas dentro del marco de la Red Iberoamericana de Protección de Datos, reuniendo a nueve países pertenecientes a dicha organización, en su calidad de miembros, asociados u observadores, representados por seis instituciones de ámbito nacional y provincial, al Instituto Federal de Acceso a la Información y Protección de Datos (Presidencia de la RED), a la Agencia Española de Protección de Datos (AEPD, Secretaría Permanente de la RED) y a expertos de asociaciones civiles y empresas multinacionales del sector privado. En total se presentaron un total de veinte intervenciones de países, instituciones (Portugal no estaba) y de asociaciones y empresas del sector privado, conforme al programa diseñado previamente.

El acto inaugural fue presidido por Dña. Lidia Blanco, Directora del Centro de Formación de la Cooperación Española, D. Carlos Andrés de Hart Pinto, Viceministro de Desarrollo Empresarial de Colombia, D. Jesús Rubí Navarrete, Adjunto al Director de la Agencia Española de Protección de Datos, y Dña. María Marván Laborde, Comisionada del Instituto Federal de Acceso a la Información y Protección de Datos.

El primer día del seminario comenzó con la exposición del marco normativo de las transferencias internacionales y de sus excepciones en la LOPD. Se estudiaron las cláusulas contractuales tipo como instrumento de las empresas para solicitar autorizaciones de transferencias internacionales de datos. A continuación se examinó la evolución de los movimientos internacionales de datos inscritos en el Registro General de Protección de Datos y de las autorizaciones otorgadas por el Director de la Agencia, destacando las 378 transferencias declaradas a Argentina a fecha de 31 de marzo de 2011.

En las siguientes ponencias se examinó la incidencia de las modalidades de transferencia internacional de datos en las corporaciones multinacionales. En primer lugar, Telefónica expuso su estructura societaria (Telefónica España, Telefónica Latinoamérica, Telefónica Europa) y expuso su modelo de atención al cliente. Las transferencias internacionales tienen su razón de ser, en este caso, en la necesidad de prestar un servicio

global con gran movilidad laboral, de reducir costes y es en definitiva una apuesta por subcontratar servicios a empresas localizadas en Latinoamérica (Colombia, Perú, Argentina Chile, Paraguay y Guatemala).

Nextel México es una empresa de origen estadounidense, pero tiene gran presencia en países de Latinoamérica: Argentina, Perú, Chile, Brasil y México y ha tenido que adaptarse a la Ley Federal de Protección de Datos Personales en Posesión de Particulares, para lo cual se realizó una auditoria. Actualmente no realiza transferencias internacionales de datos personales de sus suscriptores, sin embargo en el futuro existe un proyecto que en caso de concretarse se concentraría toda la información de sus suscriptores en Estados Unidos de Norteamérica.

El BANCO BILBAO VIZCAYA ARGENTARIA S.A. (BBVA) realiza con carácter general transferencia de datos a países con el mismo nivel de protección, pero aboga por la flexibilidad optando por la posibilidad de transferencia de datos a otros estados que no ofrezcan el mismo nivel de protección cuando el destinatario se comprometa a ese nivel de protección a través de cláusulas contractuales apropiadas. Incluso cuando las transferencias se lleven a cabo en el seno de grupos multinacionales, la garantía consistiría en normas internas de privacidad de carácter vinculante. Defiende el acercamiento del modelo de TID al de las redes sociales y del cloud computing, a través de un modelo con mayor flexibilidad/creatividad y menos formalismo.

Hewlett Packard es una empresa que opera globalmente y ha optado por un modelo de protección de Datos a nivel mundial con el fin de simplificar flujos internacionales y que responda a su responsabilidad social y accountability. Existen varios mecanismos para permitir las TID: contratos modelo, regulaciones, Acuerdo de puerto seguro. Defiende que las empresas también pueden facilitar las TID a través de acuerdos intercompañía, contratos y políticas globales. Las soluciones para el futuro que propone son regulaciones que obliguen a 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).

Posteriormente, en el siguiente panel se examinaron las TDI desde la perspectiva de los países latinoamericanos. CORFO es una agencia gubernamental que apoya el desarrollo económico de Chile, identificó los servicios globales en la industria del offshoring: ITO, BPO, KPO, donde el consumidor del servicio está fuera del país de producción. 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.

La Asociación Nacional de empresarios de Colombia (ANDI), agrupa a empresas del sector industrial, financiero, de alimentos, comercial, textil y de servicios. ANDI presentó un estudio comparativo de cómo había evolucionado el mundo de los negocios en las dos últimas décadas, estando en la actualidad en la cuarta generación de outsourcing.

La primera jornada finalizó con el examen de las modalidades de transferencia internacional de datos y su incidencia en la eficacia para realizarlas, comenzando por el examen de las Decisiones de Adecuación de la Comisión Europea de conformidad con la Directiva 95/46/CE. Se expusieron los criterios de adecuación del Grupo de Trabajo del artículo 29 de la Directiva y del procedimiento para llevarlo a cabo, aludiendo a un posible cambio en la normativa europea en los mecanismos de transferencias internacionales.

A continuación, se abordó el tema de las cláusulas contractuales tipo para transferencias a encargados de tratamiento en terceros países, tal y como se recoge en la Decisión de la Comisión 2010/87/UE. En la actualidad existe un interés creciente en promover el uso de estas cláusulas a terceros países que no ofrezcan un nivel adecuado de protección, actualizar las cláusulas para abordar nuevos problemas, y finalmente, establecer cláusulas para subencargados del tratamiento.

La ponencia de Hewlett – Pakard se centró en las normas corporativas vinculantes BCR'S, según su modelo global al que se hizo referencia en los párrafos anteriores.

Finalmente, se abordó el modelo de CBPR's según el modelo de APEC en su aplicación por MetLife. En este supuesto, los Reglamentos de datos personales de Estados Unidos requieren que las empresas adopten controles administrativos, técnicos y físicos según el tamaño de la empresa para evitar el riesgo de sobrerregulación. MetLife compartió sus principios corporativos de privacidad y su modelo de protección contra la pérdida de datos.

La segunda jornada se inició con los instrumentos para la aplicación de la normativa de protección de datos. La Agencia Española de Protección de Datos explicó las políticas preventivas llevadas a cabo, tales como las consultas de los ciudadano (presenciales, telefónicas, telemáticas y la divulgación de las guías) las consultas al gabinete jurídico, los seminarios organizados en la Agencia y las reuniones con las empresas. En cuanto al apartado de la autorregulación, se examinó la regulación de los códigos tipo, su tipología y los supuestos prácticos que han supuesto su inscripción en el Registro General de Protección de Datos. En materia de "enforcement", se examinó el volumen de las inspecciones, denuncias, sanciones y tutelas de derechos de conformidad con los datos de la Memoria del año 2010.

La experiencia de Telefónica en políticas preventivas se centra en la grabación de las contrataciones, en la instalación y entrega de los terminales solo a los titulares. En cuanto a los envíos publicitarios se establece como obligación la consulta de las Lista Robinson. Los clientes de Telefónica disponen de una web de protección de datos y el personal está formado en dicha materia. En el ámbito de autorregulación, se analizó el Código Tipo de Protección de Datos de Telefónica de España.

El Instituto Federal de Acceso a la Información y Protección de Datos se propone crear una cultura de protección de datos a través de estudios de impacto, difundir estudios sobre la materia, crear un sistema de gestor de casos para ejercitar los derechos ARCO. En materia de

autorregulación la Ley Federal prevé la adopción de códigos tipo y sellos de confianza. Se explicó el procedimiento de protección de derechos, el procedimiento de conciliación y el procedimiento de imposición de sanciones, incluyendo los tipos penales.

La siguiente ponencia versó sobre los instrumentos para la aplicación de la normativa de protección de datos en la perspectiva de los países latinoamericanos. En México la LFPDPPP reconoce los derechos de tercera generación, en particular la autodeterminación informativa. Uno de los principales desafíos es la elaboración del reglamento.

La experiencia de Uruguay de acuerdo con la Agencia de Gobierno Electrónico y Sociedad de la Información comenzó por una exposición pormenorizada de su normativa y de los pasos que llevaron a su declaración como país adecuado. Se analizaron las bases de datos inscritas, las denuncias, consultas y sanciones impuestas durante el año 2010.

En la actualidad, Colombia cuenta con una legislación penal Ley 1273/2009 de tipificación de conducta por violación de datos personales, y con la Ley 1266/2008 para el sector comercial, financieros, servicios y de datos provenientes de terceros países, siendo el objetivo alcanzar el nivel adecuado por parte de la Unión Europea, para lo cual se ha aprobado una Ley sobre protección de datos personales.

En países como Costa Rica donde al día de hoy no cuentan con una Ley de Protección de Datos y se ha hecho uso de normas dispersas (Constitución Política, Convención América de los Derechos Humanos entre otros) estando fraguándose una regulación sobre la materia. Muchas Instituciones Públicas han tomado conciencia y se han limitado el acceso al uso irrestricto de la información que descansa en sus bases de datos.

El siguiente panel abrió el debate de los instrumentos de autorregulación. La Secretaría de Economía estudió el perfil de dicho país, y expuso la encuesta en materia de protección de Daros realizado a PYMES.

Asimismo, se examinó la autorregulación en la Ley de Protección de Datos Personales en Posesión de los Particulares de México, a través de esquemas de autorregulación que se notifican ante la autoridad sectorial y al IFAI, siendo compatibles con las CBPR's y BCR's.

En Uruguay, la autorregulación cuenta con los siguientes instrumentos: códigos de conducta de práctica profesional, directivas de protección de información personal, códigos de autorregulación, códigos de deontología y códigos tipo, que incluyen normas de seguridad, sellos de calidad, solución arbitral de las controversias y sanciones por incumplimiento.

En la sesión de tarde el debate se centró en las experiencias sectoriales de autorregulación. Comenzó el IFAI exponiendo los lineamientos de protección de datos personales, las verificaciones, las capacitaciones y los impactos a la privacidad.

La Agencia Española de Protección de Datos expuso las responsabilidades en materia de protección de datos en los ensayos clínicos con medicamentos, y los mecanismos de aplicación del código tipo adoptado.

El panel finalizó con la exposición de la Asociación Mexicana de Internet del proyecto de Sellos de Confianza AMIPCI®, como mecanismo de autorregulación en materia de privacidad, enfocado principalmente a la actividad comercial digital.

Las últimas intervenciones se centraron en exponer otros instrumentos preventivos en la aplicación de la normativa de protección de datos personales. En concreto, la Agencia Española de Protección de Datos expuso las Inspecciones Sectoriales llevadas a cabo en los últimos años (en hospitales, Internet, publicidad telefónica, enseñanza, etc.).

La última intervención la realizó un representante de Google quien expuso su política de privacidad de empresa, sobre todo ante los nuevos retos de las redes sociales y cloud computing, para terminar por hacer referencia a las modalidades de TID que realiza dicha empresa a nivel global.

En la última jornada se celebró una reunión cerrada de la RED, en la que se debatieron propuestas de recopilación de jurisprudencia en materia de protección de Datos, de participación en los trabajos sobre protección de datos de la Organización de Estados Americanos (OEA), se presentaron las líneas generales de la Conferencia Internacional que se celebrará en México, y se abordó la celebración del IX Encuentro en dicha Conferencia.

El acto de clausura sirvió como colofón a tres días intensos de debate y reflexión sobre el impacto y regulación de las transferencia internacionales, la deslocalización de actividades económicas en América Latina, las experiencias de los países de la Red en políticas preventivas, autorregulación y enforcement, experiencias sectoriales de autorregulación, y otros instrumentos preventivos en la aplicación de la normativa de protección de datos

El Seminario ha dado continuidad a los trabajos de la Red Iberoamericana de Protección de Datos, potenciando así las iniciativas de intercambio de experiencias entre los países iberoamericanos y estableciendo canales abiertos de diálogo y colaboración en materia de protección de datos personales.

En Cartagena de Indias, a 16 de junio de 2011.