SEMINARIO "NUEVAS TECNOLOGÍAS: SEGURIDAD VS PRIVACIDAD"

Durante los días 21 a 23 de julio de 2010, 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, el "Seminario Nuevas Tecnologías: Seguridad vs. Privacidad". Como una de las actividades aprobadas dentro del marco de la Red Iberoamericana de Protección de Datos para el año 2010, en esta ocasión se han congregado 15 países miembros, representados por 36 instituciones de ámbito nacional y provincial, una representante del Supervisor Europeo de Protección de Datos, del Cuerpo Nacional de Policía de España y a expertos de asociaciones civiles y del sector privado (Google, Yahoo! y Telefónica). En total se presentaron un total de veintiocho intervenciones, conforme al programa diseñado.

El acto inaugural fue presidido por **Dña. Claudia Ramírez,** Viceministra de desarrollo empresarial, del Ministerio de Comercio, Industria y Turismo de Colombia, **D. Artemi Rallo,** Director de la Agencia Española de Protección de Datos (AEPD), **D. Gustavo Valbuena,** Superintendente de Industria y Comercio de Colombia y **Dña. Lidia Blanco,** Directora del Centro de Formación de la AECID en Cartagena de Indias.

La Viceministra Ramírez destacó la importancia de aprobar una Ley General de Protección de Datos en Colombia, informando de la reciente presentación en el Congreso de un proyecto legislativo en materia de protección de datos. Mencionó el volumen de retos que en la actualidad su país debe asumir en esta materia así como la importancia de estas actividades en el marco iberoamericano. El Superintendente Valbuena recalcó los avances normativos experimentados en el último año en Colombia y su efecto económico sobre el incremento competitivo de este país a nivel internacional, garantizando la protección de datos personales junto a la apertura de negocios en el sector de las telecomunicaciones y la implantación de tecnologías de la información. El Director de la AEPD destacó la importancia de esta cita anual que permite compartir los diferentes avances a nivel normativo que han experimentado algunos países de la región como Perú, Panamá, Chile o República Dominicana, junto a los éxitos ya alcanzados de Argentina, Uruguay o México, que deben servir como una motivación para el resto de países que todavía no han aprobado una ley general en la materia. El Director recordó las actividades previstas para el año 2010, así como la convocatoria de la Conferencia Internacional de Autoridades de Protección de Datos del próximo mes de octubre en Jerusalén. Finalmente, hizo referencia al desarrollo de las realidades que se analizarían durante el seminario que junto a ciertas preocupaciones y riesgos, fruto de la globalización, deben conciliarse junto al equilibrio de derechos fundamentales como el derecho a la privacidad.

El primer panel que abrió el seminario abordó el tema de la **"Seguridad y Privacidad en el marco de las Telecomunicaciones",** comenzando el Superintendente de Industria y Comercio de Colombia con un análisis detallado del régimen colombiano de protección de datos personales (inviolabilidad de las comunicaciones, seguridad de los datos, mensajes comerciales o publicitarios y el régimen sancionador) y de las competencias de la Superintendencia en materia de telecomunicaciones. La representante de Telefónica resaltó el incremento del número de prestadores de servicios, frente a consumidores más conocedores de sus derechos. Si bien es cierto que Internet favorece la proliferación de contenidos y facilita menos accesos a la información, también surgen nuevos retos que afectan a la privacidad. Actualmente existe un procedimiento regulado en caso de violación de datos personales que establece una serie de obligaciones explícitas que debe cumplir el prestador de comunicaciones electrónicas junto a los principios generales de consentimiento previo, una amplia legitimación activa, así como la posibilidad de imponer sanciones a dichos prestadores. Se analizaron las novedades incorporadas en

las últimas Directivas Comunitarias en materia de comunicaciones electrónicas y los principales retos que en materia de privacidad tienen los operadores de telecomunicaciones. Se mencionaron los cuatro principios (libertades) que rigen en materia de protección del derecho a la propiedad intelectual y la neutralidad en la red, recordando que las medidas limitadoras deben ser proporcionadas y sujetas al principio de tutela judicial efectiva, siendo necesaria en todo caso una norma con rango de Ley en lo referente a las medidas garantes del libre ejercicio de la propiedad intelectual.

El representante del IFAI destacó los pilares fundamentales relacionados con la seguridad de la información, como son la proporcionalidad, la integridad y la finalidad, resaltando la necesidad de aprobar medidas de seguridad adecuadas a la transmisión de datos así como la de identificar los datos que han de ser tratados y conservados posteriormente. La intervención de Yahoo! realizó un breve análisis de la evolución de la entidad en materia de privacidad y transparencia, explicando la estructura de su entidad y las medidas de control y protección de la privacidad de los usuarios que han implementado. Resaltaron la transparencia del sitio Web cuando su objetivo es presentar una amplia oferta de servicios, siendo conscientes de las continuas actualizaciones que deben implementar ante al fenómeno de las redes sociales. Finalmente se expusieron distintos proyectos que la entidad ha desarrollado, como Ad Icon, así como la idea de la publicidad personalizada y la experiencia social de compartir información pública en Yahoo!.

La segunda parte de la jornada se dedicó a la **"Seguridad y protección de datos en el sector financiero".** Uruguay expuso la actividad y funcionamiento de las Unidades de Inteligencia Financiera. El ejercicio de los derechos ARCO y la financiación en el marco de las investigaciones sobre el lavado de activos fueron cuestiones que se abordaron y ampliaron con casos jurisprudenciales, dejando abierta la pregunta de quién controla al controlador. También hubo lugar para conocer el marco regulatorio chileno así como el sistema de información financiero y los procesos de comunicación establecidos, identificando la problemática vinculada a la protección de datos personales y a la transparencia del mercado financiero. Posteriormente correspondió el turno al Superintendente Financiero de Colombia, quién analizó la normativa colombiana vigente junto a la estructura, funcionamiento y competencias de la Superintendencia, identificando una serie de riesgos para la protección de datos como: las infidelidades internas respecto al tratamiento de datos, la tercerización de servicios, la captura ilegal de datos o la implantación y uso inadecuado de las nuevas tecnologías. Los retos del sistema financiero se centran en mantener la protección de un número creciente de datos personales, garantizar el acceso de los titulares a la información en los operadores de bancos de datos y fuentes, mantener actualizada la información, garantizar la confidencialidad e integridad de la información manejada por terceros y la procesada en otros países así como administrar los riesgos que conllevan el uso de nuevas tecnologías.

La jornada finalizó con el panel de intervenciones titulado: **"Seguridad y protección de datos en el transporte aéreo".** En esta sección se expusieron los diferentes acuerdos internacionales en materia de intercambio de información de pasajeros así como el tipo de datos transmitidos bajo este tipo de acuerdos. Por parte del IFAI y del Instituto de Transparencia del Estado de Aguas Calientes (México), se analizó el cumplimiento de los principios generales de protección de datos así como el ejercicio de los derechos ARCO a la luz de la implantación de tales acuerdos y sistemas. Una vez más se aludió a la necesidad de impulsar normativas reguladoras del tratamiento de datos personales en América Latina a través de legislaciones concretas. Por parte de la AEPD se analizó esta temática desde la perspectiva de la

implantación de escáneres corporales, sus finalidades, el papel de las autoridades, los diferentes sistemas de acceso a la información, así como el tratamiento de datos sensibles que conlleva la implantación de los mismos. Citando la actual Comunicación de la Comisión al Parlamento Europeo, que establece la necesaria aplicación de los principios de proporcionalidad y finalidad, se mencionaron posibles vías para la protección de la dignidad humana, los datos personales u otros derechos fundamentales. También se analizaron los diferentes sistemas de seguridad, manual o electrónicos a la luz del principio del consentimiento previo al tratamiento de la información personal, finalizando la intervención con una exposición del sistema de control de acceso a zonas restringidas de seguridad que se pretende implantar en los aeropuertos españoles y las repercusiones de dicho sistema, dentro del programa nacional de seguridad, sobre la normativa de protección de datos.

Durante la segunda jornada del seminario se abordó el tema de la **"Criminalidad en la Red"**, comenzando por analizar la relación entre la ciberdelincuencia y la privacidad. Posteriormente se expuso el fenómeno de la "Cloud Computing", sus modalidades, aplicaciones, contextos, beneficios (tanto en lo que afecta al acceso a la última tecnología como a la mayor seguridad e innovación) y sus controversias (alta dependencia del proveedor de servicios, integridad, seguridad y privacidad de los datos, aspectos referentes a los derechos de autor de la información, falta de una regulación explícita). A continuación, el representante de Google presentó los principios y herramientas que su entidad facilita a los titulares de los datos para controlar sus datos personales así como los desafíos regulatorios que nos obligan a re-pensar sobre conceptos de privacidad. Dentro del mismo panel pudo conocerse una amplia tipificación de los diferentes delitos que pueden cometerse a través de la red: Phising, Bullying, Pharming, Scam, Grooming, Scavenging. La colaboración ciudadana es considerada una herramienta muy útil para las Fuerzas y Cuerpos de Seguridad que combaten estas categorías delictivas. Además se expuso la normativa uruguaya junto al procedimiento de investigación y la actuación de las autoridades competentes, destacando el rol de AGESIC y su compromiso con la seguridad de la información, partiendo de la protección de los datos personales, como impulsores de la ley vigente y trabajando en la gestión y consolidación del derecho, así como en la salvaguarda de los activos críticos de información del Estado.

La segunda parte de la jornada la protagonizaron los paneles dedicados a la "**Seguridad y Privacidad en los movimientos migratorios",** analizándose por parte de la representante del Supervisor Europeo, el marco legislativo actual, desde la transposición de la Directiva 95/46 CE, el Programa de Estocolmo, los Acuerdos Schengen y el régimen de supresión y armonización de controles fronterizos junto a los nuevos instrumentos electrónicos implantados, los cuáles facilitan la circulación de personas al mismo tiempo que controlan los plazos autorizados de permanencia en una región. Desde dicha institución se incide en la necesaria evaluación de los sistemas existentes a fin de identificar posibles mejoras en su funcionamiento. El IFAI (México) destacó la necesaria ponderación de los derechos fundamentales en el ámbito de la protección de los datos de migrantes y refugiados, donde en ocasiones se mezcla el interés público con el interés estatal, siendo cuestionable en algunos casos la necesidad de publicidad de la información en aras de contribuir al ejercicio de rendición de cuentas por parte de las instituciones públicas en detrimento de la protección de la privacidad. Desde el Instituto Estatal de Acceso a la Información Pública de Oaxaca (México) se analizó el fenómeno migratorio desde un punto de vista histórico, analizando las motivaciones y restricciones que afectan al mismo, destacándose los efectos de las redes sociales en la comunidad de origen de los migrantes en el sentido de facilitar la comunicación y las relaciones sociales. Se insistió en la necesaria promulgación de normas efectivas de protección de datos así como acuerdos entre México y EEUU que garanticen los derechos de los migrantes.

La representante del Tribunal Electoral de Panamá expuso la normativa nacional en materia de acceso a la información pública, planteando la existencia de interrogantes en lo referente a la seguridad y privacidad, siendo consciente de la idiosincrasia y de la diferente problemática que caracteriza a cada país. Desde el Instituto Coahuilense de Acceso a la Información Pública se hizo una exposición recalcando la necesaria congruencia entre los derechos de seguridad, libertad y libre tránsito, haciendo alusión a la necesaria cooperación a la hora de organizar los movimientos migratorios. La seguridad personal y ciudadana junto al respeto a la privacidad han de conjugarse con la garantía de movimientos migratorios ordenados.

La jornada finalizó con el panel dedicado a la **"Protección de Datos y la Cooperación Policial Judicial",** interviniendo un representante del órgano Judicial de Panamá, quién compartió con los asistentes la normativa panameña al respecto y destacando entre las finalidades de la cooperación policial judicial el cumplimiento de la ley, el respeto por la dignidad humana y la protección de los derechos humanos. A continuación, en representación de la Corte Superior de Justicia de Lima, se realizó una intervención destacando los principios de verdad procesal y las posibles situaciones conflictivas que pudieran aparecer debido a la preeminencia de determinadas autoridades o de la ineficacia del sistema administrativo judicial vinculado al tratamiento de datos. Se identificaron los agentes protagonistas así como el objeto primordial de la cooperación policial y judicial (investigación de hechos e identificación de personas), las diferentes formas de regulación y los alcances de la cooperación policial y judicial, concluyendo con la necesidad de alcanzar una efectiva protección de los datos ante los diferentes tratamientos realizados por las autoridades nacionales y la falta de una normativa que regule la materia. Por parte de Colombia intervino un juez de Control de Garantías Constitucionales, quién además de mencionar varios textos normativos vigentes, expuso una serie de casos reales de intromisión a la privacidad resueltos por el Consejo de Estado. Finalizando la jornada intervino una representante de la Corte Superior de Justicia de Paraguay, quién aludió a las bases de datos de procesos penales, la legitimación de aceso a la información privada así como las funciones de la Oficina de Estadísticas Penales y la Oficina de Antecedentes Judiciales y sus procedimientos de actuación reglamentados, citando algunas disposiciones específicas sobre el manejo de datos por parte del Poder Judicial y destacando que la interoperabilidad entre el Poder Judicial y la Policía Nacional se circunscribe exclusivamente a la base de datos identificativos de las personas físicas. En último lugar intervino la AEPD, realizando una exposición que partía de la mención de la normativa europea (tratados y directivas actuales) que han resuelto la implantación del Sistema de Información Europeo de Antecedentes Penales (ECRIS), haciendo alusión a la existencia de acuerdos bilaterales y multilaterales y al documento sobre modelos de cláusulas que la Comisión Europea ha redactado a fin de recordar la necesaria observancia de los principios de protección de datos a la hora de firmar este tipo de acuerdos.

La última jornada del seminario se dedicó al panel titulado **"Tecnología avanzada frente a la limitación de la privacidad",** iniciando la serie de intervenciones el representante del Registro Nacional de Costa Rica, quién tras realizar un breve balance de los derechos individuales y de la colectividad en Costa Rica, mencionó los efectos sociales y la problemática surgida a raíz del uso de dispositivos tecnológicos de videovigilancia pública, identificando las relaciones existentes entre las diferentes instituciones y el Gobierno así como entre el Poder Ejecutivo y la Sociedad Civil. La licitud del uso de la imagen personal por parte de la Policía ha de estar ligada a la investigación del delito, debiendo en caso contrario establecer el uso restringido de los sistemas de videovigilancia. Por parte del Ministerio de Ciencia y Tecnología de Brasil, se mencionó la normativa específica que regula los sistemas de identificación automática en este país, siendo conscientes de

que la falta de una norma de protección de datos puede llevar en ocasiones a una vulneración de la intimidad en este ámbito. Otro de los temas que se trató fue el registro de acceso a los servicios de Internet y la necesidad del consentimiento previo, libre e informado respecto al tratamiento de datos personales. Finalmente intervino la representante del Supervisor Europeo de Protección de Datos, quién analizó las recomendaciones del Supervisor en materia del uso de dispositivos RFID (identificadores por radiofrecuencia), mencionando sus diferentes utilidades y los riesgos que pueden entrañar para la privacidad. Terminó su intervención haciendo mención al presente y futuro del diálogo entre el regulador y la industria, considerando los documentos del Grupo de Trabajo del Artículo 29 y de la Agencia Europea de la Sociedad de la Información (ENISA), quiénes se mantienen cautelosos ante el uso de tales dispositivos sin un previo análisis de las medidas de seguridad y de los riesgos para la privacidad que deberían considerarse antes de su implantación global.

El acto de clausura fue presidido por la Directora del Centro de Formación, Lidia Blanco, quién destacó el ejemplo de la Red Iberoamericana como foro de intercambio de experiencias y evolución en los últimos años que permite avanzar en las materias comunes que comparten las instituciones iberoamericanas que forman parte de esta Red. El Adjunto al Director de la AEPD, Jesús Rubí, comenzó destacando la buena salud de que goza la Red Iberoamericana, una Red que no es exclusivamente de la AEPD, sino que abarca a toda la región iberoamericana, la cuál ha experimentado avances legislativos importantes en los últimos años, una presencia institucional cada vez mayor así como la proyección del Derecho Fundamental a la protección de datos en la agenda y en los debates de los distintos países iberoamericanos, algunos de los cuáles ya han iniciado sus procesos de adecuación. Considerando que el Habeas Data ha alcanzado la mayoría de edad, destacó que las leyes de protección de datos han reflejado una protección transversal de los ciudadanos en las más variadas áreas de actividad. Se trata en definitiva de un fenómeno que se retroalimenta, destacando los avances normativos que se producen en cada país y que permiten trasladar el debate a la protección efectiva, ampliándose su actividad a terceros países. Junto a la proyección considerable que ha alcanzado la Red, no hay que olvidar la necesidad de seguir avanzando y consolidar la presencia institucional de cada país miembro, extendiendo los resultados de las actividades celebradas dentro del marco de la Red a los diferentes países y potenciar las herramientas comunes. Finalmente agradeció la colaboración de la AECID y de las instituciones participantes, emplazando a todos los miembros de la Red al próximo Encuentro Iberoamericano que se celebrará en la ciudad de México los días 29 y 30 de septiembre.

En Cartagena de Indias, a 23 de julio de 2010.