SEMINARIO REGIONAL DE PROTECCIÓN DE DATOS

Durante los días 1 al 4 de junio 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 Montevideo, el "Seminario Regional de Protección de Datos". En esta ocasión el evento se ha dirigido especialmente a los países que en la actualidad forman parte del MERCOSUR, como una de las actividades aprobadas dentro del marco de la Red Iberoamericana de Protección de Datos, reuniendo a los 11 países pertenecientes a dicha organización, en su calidad de miembros, asociados u observadores, representados por 32 instituciones de ámbito nacional y provincial, a la Comisión Nacional de Protección de Datos (CNPD), de Portugal, a la Agencia Española de Protección de Datos (AEPD) y a expertos de asociaciones civiles y del sector privado. En total se presentaron un total de cuarenta intervenciones, conforme al programa diseñado previamente.

El acto inaugural fue presidido por la embajadora de España en Uruguay, Dña Aurora Díaz-Rato, D. Jesús Maestro, Director del Centro de Formación de la AECID, D. Luis Lingnau da Silveira, Presidente de la CNPD, D. José Clastornik, Director Ejecutivo de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), de Uruguay, D. Raúl Urrutia, Presidente del Consejo para la Transparencia de Chile y D. Rafael García, Jefe del Área Internacional de la AEPD.

El primer día del seminario se dedicó a las Transferencias Internacionales de Datos, dirigidas a países con nivel o no adecuado de protección de datos. Se expusieron las diferentes fases que conforman el proceso de adecuación ante la Comisión Europea y se hizo mención especial a la regulación internacional y nacional de varios países, haciéndose hincapié en los diferentes procesos de adecuación existentes así como en los requisitos, objetivos y criterios que se regulan en la normativa procedente de la Comisión Europea. Desde un punto de vista práctico se citaron algunos de los aspectos más relevantes que han tenido como protagonistas a los países inmersos recientemente en el mencionado proceso de adecuación.

La importancia del conocimiento de la normativa de protección de datos personales por parte de los ciudadanos y la empresas se considera imprescindible, no sólo en el sentido de hacer valer sus derechos y obligaciones sino también en el camino de una mayor concienciación y difusión de este Derecho Fundamental.

Se mencionaron las cláusulas contractuales tipo y las Binding Corporate Rules (BCR´s), exponiéndose las ventajas y posibles inconvenientes que pudiera tener su utilización así como su compatibilidad con el ordenamiento jurídico nacional de los países iberoamericanos. La trayectoria y la experiencia adquirida desde la aprobación del Acuerdo de "Safe Harbour", hace ya diez años, permitió recordar las diferentes obligaciones que deben cumplir las compañías exportadoras de datos personales así como las consecuencias de su incumplimiento, según la normativa aplicable en cada caso concreto.

En la segunda jornada se expusieron diferentes paneles relacionados con la armonización entre las leyes de transparencia y los estándares internacionales de protección de datos personales, destacándose el papel privilegiado del Estado como responsable del tratamiento de datos personales, el cuál debe actuar con extrema precaución a la hora de realizar una comunicación de datos. La acreditación del interés legítimo ocupa una posición primordial a la hora de ponderar entre el acceso a la información pública y la protección de datos personales, siempre salvaguardando las excepciones reguladas por la Ley.

En el mismo panel se expusieron los diferentes sistemas y modalidades de ejercicio de acceso a la información pública y los métodos y procedimientos que las diferentes instituciones nacionales tienen implementados para satisfacer dichas solicitudes. El Gobierno interconectado, como Gobierno en Red, es una de las calificaciones que identifica a ciertos Ejecutivos iberoamericanos. La circulación y el flujo de información personal obliga por otro lado a garantizar una necesaria y efectiva protección de los datos personales.

La Interoperabilidad y su incidencia en la Privacidad, dentro del marco de las Administraciones Públicas, ocupó el tema central de la segunda parte de la jornada, siendo la obtención de datos entre administraciones una tarea muy necesaria pero en muchas ocasiones bastante ardua, en el sentido de tener que conjugar tanto aspectos jurídicos, económicos, políticos

como tecnológicos. Esta labor puede chocar con la verdadera eficacia de los organismos públicos, que en muchas ocasiones se ven en la obligación de justificar su legitimación para obtener determinada información personal que les permita desarrollar sus competencias de una manera eficaz. La gestión pública eficiente exige conocer a quién va dirigida la misma, de ahí que sea necesaria nuevamente la ponderación entre el acceso a la información pública y la privacidad.

Principios como la “ventanilla única” se van implantando en las diferentes administraciones dentro del marco de la percepción unitaria del Estado. Se trata en definitiva de lograr modelos de Estado compatibles con los Derechos Humanos, que permitan una ponderación y una defensa equilibrada de los derechos e intereses en juego. En muchas ocasiones el excesivo celo por los datos impide una mayor eficacia de la Administración. El flujo de información debe conocer de unas limitaciones, sin embargo al hablar del Derecho Público debemos considerar un Derecho abierto, transparente, donde la Administración se caracterice por su Eficacia, Eficiencia, Economía y Ética sin olvidar la observación y cumplimiento de principios como la finalidad o el consentimiento previo informado, los cuáles ocupan un lugar primordial en materia de protección de datos personales.

Desde una perspectiva conciliadora y no conflictivista la privacidad y la interoperabilidad pueden convivir pacíficamente. La interoperabilidad ha de definirse como un instrumento y no como un fin, de ahí que haya que defender una necesaria circulación de información entre Administraciones, considerando la protección, eso sí, de la información privada frente a la libre circulación y sin límites de la misma. La Ley es la fuente de obrar de las Administraciones y no su límite, predicándose la libertad no de la Administración sino de los ciudadanos. La disponibilidad, la accesibilidad y la integración son características que definen al Gobierno Electrónico, identificando como tangible al derecho a la información pública. La documentación electrónica en el marco de la interoperabilidad de un Gobierno electrónico exige para su adecuado desarrollo asegurar a las personas una autenticidad, una integridad y en todo caso cualquier ausencia de repudio, debiendo el Estado asumir sus responsabilidades como tenedor de la información personal y obligado a implementar las medidas de seguridad correspondientes al tipo de datos tratados.

La externalización de servicios en determinados procesos de negocios ha supuesto en materia de transferencias internacionales un crecimiento digno de mención, en cuyo ámbito algunas organizaciones públicas y privadas son conscientes de que la reducción de costes que permite el aumento de estas actividades no debe menoscabar la importancia del cumplimiento de una normativa de protección de datos y en concreto la implantación de las medidas de seguridad correspondientes que garanticen el uso adecuado de los datos personales.

Las últimas intervenciones del día aludieron a los Derechos Humanos, cuya indivisibilidad e interdependencia se recalcaron con especial interés, siendo conscientes de que el derecho a la protección de datos pese a su naturaleza autónoma, multifacética y solidaria, puede en ocasiones considerarse como el límite legítimo al ejercicio de otros derechos, como la libertad de expresión, el derecho de acceso a la información o la libertad de información. Siendo conscientes de los riesgos y problemas que se asumen al vivir en una sociedad vigilada no por ello hay que renunciar al desafío de lograr un sistema normativo garante y protector de un derecho fundamental como la protección de datos personales que se consolide a través de la implantación y aplicación de principios como la legalidad, la información previa a recabar el consentimiento de su titular, la calidad, la seguridad, la finalidad y la proporcionalidad.

Las conferencias que ocuparon el tercer día del seminario se centraron en exponer una temática en cierto modo controvertida, en el sentido de revelar la doble condición de los jueces como responsables de organismos jurisdiccionales, que deben velar por la protección de los derechos reconocidos en la legislación vigente así como responsables de ficheros y tratamientos de datos personales. Se conocieron las normas sectoriales aprobadas y las diferentes categorías de datos que reconoce la normativa y la jurisprudencia nacional, cuyas interpretaciones de las leyes vigentes en ciertos casos resulta muy dispar. El tratamiento de datos sensibles se analizó desde diferentes ordenamientos jurídicos afectados por las vicisitudes políticas de cada momento, siendo en muchos casos los Derechos Humanos los más vulnerados. En este sentido, las leyes de transparencia administrativa se han definido como leyes que reglamentan la información privada.

El tratamiento de datos personales en el ámbito de la justicia digital ha permitido desvelar la tensión generada con la privacidad por parte de las TIC,s. El principio de publicidad procesal fue muy debatido desde la perspectiva del necesario balance que han de considerar los órganos judiciales a la hora de ponderar entre la publicidad de las resoluciones y sentencias y la protección de la privacidad. Las reglas de Heredia, aprobadas en Costa Rica en el año 2003 fueron mencionadas en varias ocasiones a efectos de clarificar la posición prioritaria de la privacidad que de las mismas se desprende. La incorporación de la tecnología no debe menoscabar la protección de la privacidad, siendo necesaria una armonización de las reglas de acceso a la información así como la aprobación de unos estándares de protección mediante mecanismos transparentes, permitiendo la participación de los actores sociales afectados. Las garantías en el acceso a la información y la protección de datos personales en el ámbito jurisdiccional fue una materia que se abordó en dos paneles diferentes y que permitieron a los asistentes conocer una amplia casuística en este ámbito.

La regularización internacional de los Bureau de información crediticia y el tratamiento de datos sensibles en las empresas, considerando la especial incidencia del secreto profesional fueron los temas protagonistas de la última jornada del Seminario, donde se pudieron conocer diferentes sistemas de tratamiento de datos correspondientes a deudores de entidades financieras y su compatibilidad con la protección de datos personales, así como los diferentes tipos de ficheros (positivos y negativos) que dichas entidades pueden manejar.

Desde el punto de vista empresarial, la globalización y los avances tecnológicos exigen un alto nivel de la calidad de los servicios prestados, máxime en un mercado donde la externalización de éstos se ha convertido en una práctica habitual, la cuál no debe olvidar las distintas relaciones que surjen, desde el punto de vista de la protección de datos, entre responsable del fichero y el encargado del tratamiento.

Los derechos y las obligaciones, tanto de abonados como de responsables de bases de datos en el marco de las telecomunicaciones quedaron claramente expuestos, tal y como la normativa de cada país tiene regulados, diferenciándose las sanciones penales y administrativas que pueden llevar aparejadas el incumplimiento de las primeras.

La jornada se cerró con la exposición dedicada al tratamiento de datos sensibles por parte de entidades empresariales, destacándose el papel de los encargados del tratamiento frente a los responsables de bases de datos, así como la normativa sectorial aprobada en alguno de los países intervinientes.

El acto de clausura sirvió como colofón a cuatro días intensos de debate y reflexión sobre los distintos problemas que surjen en el amplio marco de la protección de datos personales y en concreto en los diferentes tratamientos realizados por los responsables y encargados de bases de datos administrativas, jurisdiccionales crediticias y empresariales, así como su repercusión en el entorno de las transferencias internacionales de datos. Una vez más los países miembros de la Red Iberoamericana han podido comprobar que pese al reconocimiento de una legislación diferente en cada ámbito nacional, los problemas y la casuística son muy similares en la región iberoamericana, donde el intercambio de información y la búsqueda de soluciones comunes nos permitirá en un futuro caminar por la misma vía y bajo el amparo de unos principios generales y unos derechos reconocidos a nivel internacional.

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 para abordar y ofrecer alternativas rigurosas a los problemas que afectan a la protección de datos personales.

En Montevideo, a 4 de junio de 2010.