Presentación Verbal hecha por Dante Negro, Director del Departamento de Derecho Internacional, ante la Comisión de Asuntos Jurídicos y Políticos sobre el documento "Estudio Comparativo: Protección de Datos en las Américas"

Martes 13 de Noviembre de 2012

La Asamblea General, mediante resolución AG/RES.2661 (XLI-O/11), solicitó al Departamento de Derecho Internacional (DDI) en junio de 2011, que elaborara un estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, inclusive las leyes, reglamentos y auto regulación nacionales, con miras a explorar la posibilidad de un marco regional en esta materia.

La CAJP en su sesión del 6 de octubre de 2011 solicitó a los Estados miembros proveer los elementos necesarios para el estudio. Las Delegaciones solicitaron la elaboración de un cuestionario por parte del DDI de manera tal que todas las respuestas siguieran el mismo formato. El cuestionario circuló entre las Delegaciones mediante el documento CP/CAJP-3026/11 el 31 de octubre de 2011. Los Estados miembros decidieron como fecha límite para la entrega de sus respuestas el 15 de enero de 2012, fecha que se extendió hasta el 15 de febrero de ese año.

Once Estados miembros respondieron al cuestionario, a saber, Argentina, Canadá, Colombia, Costa Rica, El Salvador, Estados Unidos, México, Panamá, Perú, República Dominicana, y Uruguay. El DDI agradece a todos estos Estados miembros por el interés que le pusieron al tema, lo cual ha permitió elaborar el documento CP/CAJP-3063/12 "Protección de Datos en las Américas: Un Estudio Comparativo", bastante amplio y desarrollado sobre la situación de la protección de datos a nivel interamericano.

La Asamblea General en su más reciente período ordinario de sesiones, mediante resolución AG/RES.2727 (XLII-O/12), agradeció al DDI la presentación de este documento y encomendó al Consejo Permanente, a través de la CAJP que, antes del 43 período ordinario de sesiones de la Asamblea General, prevea en su agenda el análisis de este estudio así como el del Comité Jurídico Interamericano, y considere la posibilidad de un marco regional en esta área, teniendo en cuenta la revisión en curso de otros instrumentos internacionales en la materia.

En el documento preparado por el DDI se incluye una breve explicación de los trabajos sobre la materia que hasta el momento han desarrollado algunas organizaciones internacionales tales como el Consejo de Europa, la Unión Europea, la Red Iberoamericana sobre Protección de Datos, la Organización para la Cooperación Económica y el Desarrollo y el Foro de Cooperación Económica Asia-Pacífico.

La Parte II del documento brinda una perspectiva general sobre los marcos legales existentes en la materia. La Parte III brinda un resumen de los instrumentos internacionales adoptados o que están siendo adoptados por otras organizaciones internacionales en este tema. La Parte IV describe los regímenes internos sobre protección de datos en los países que enviaron sus respuestas al cuestionario antes mencionado.

En este punto queremos destacar la importancia del tema de la protección de datos personales en nuestros días. Dicha importancia se hace más crítica cuando observamos los avances en la informática, en la medicina y la biotecnología, y en las medidas de seguridad adoptadas en la última década, por mencionar sólo algunos.

En cuanto a la informática, el flujo extensivo de la información ha desembocado en lo que denominamos hoy la "sociedad de la información" en la cual dicha información se recaba y se disemina de una manera más rápida y con mayores alcances. La información deja así de ser un instrumento para convertirse en el principal de los bienes. Los usuarios de las computadoras, a través de actos de la vida cotidiana (compras por Internet, uso de redes sociales, etc.), dejan sus rastros en todos los sitios que utilizan y van produciendo con esto un verdadero perfil con sus creencias, intereses, preferencias, etc. El mundo está siendo traducido casi en su totalidad en información en lo que podemos denominar un "espejo virtual". Esto potencialmente puede generar un uso indebido o abusivo de dicha información además del hecho de que la misma ya no ocupa un lugar físico identificable, sino que está en el espacio virtual de las redes, y puede ser usada de manera transfronteriza, en otros países con regulaciones distintas.

En cuanto a los avances de la medicina y la biotecnología, las nuevas técnicas de investigación y el cuidado médico, a través de las pruebas con ADN, crean nuevos retos para la protección de la privacidad. Dentro de la historia clínica de cada usuario del sistema de salud se encuentran datos que son parte de su esfera íntima de salud y que se refieren a enfermedades pasadas, presentes, tratamientos recibidos, medicamentos usados, adicciones –si las tiene- e información genética, entre otros. Puede además contener datos sensibles tales como raza, vida sexual o creencias religiosas.

La solución a todos estos retos radica en poder establecer un balance adecuado entre el incentivo del flujo de datos y de información regulando al mismo tiempo dicho flujo mediante requisitos de calidad de tratamiento y creando la conciencia de la protección de los datos personales al punto de lograr que todos los que trabajan con dichos datos personales se conviertan en custodios de los mismos.

Sin embargo, el significado de la privacidad y los orígenes del derecho individual a la privacidad puede variar, y como resultado de ello, las políticas y las leyes que gobiernan el derecho a la privacidad varían de país a país y de región a región.

En general, el tratamiento del tema de la protección de datos ha seguido tres grandes enfoques.

Podemos decir que el sistema europeo es el más estricto de ellos con normas que reglamentan tanto la recolección de datos personales por parte del gobierno como por parte del sector privado. El Convenio 108 del Consejo de Europa para la Protección de las Personas respecto al Tratamiento Automatizado de los Datos de Carácter Personal de 1978 fue un modelo para las legislaciones Europeas, definiendo los datos personales como "toda información relacionada con una persona identificada o identificable". Posteriormente, en 1995, la Directiva sobre Protección de Datos 95/46/CE estableció los criterios y bases legales para el establecimiento de la protección de datos en todo el ámbito de la Unión Europea La misma admite la transferencia de datos personales a países fuera de la Unión Europea sólo cuando el país de que se trate garantice un nivel de protección adecuado de los datos o si demuestra que los datos quedarán debidamente protegidos una vez que hayan sido transferidos, ampliando así la

protección a países fuera de la Unión Europea. Esto ha obligado en la práctica a países con empresas interesadas en transferir datos personales a examinar su propia legislación para satisfacer los estándares de la Unión Europea. En general pues, en la Unión Europea prima el criterio de la “protección equivalente y la protección adecuada”, mediante el cual se envían datos en la medida en que el receptor sea confiable mediante un adecuado estándar de protección de datos personales.

Debemos advertir que dado que el documento fue elaborado a inicios del presente año, no refleja los cambios normativos y de otra naturaleza que se han gestado en los últimos meses. Esto tanto respecto a la normativa nacional como la internacional.

Este es el caso de la UE. Desde hace dos años se inició en la UE un proceso de reforma de legislación en materia de protección de datos personales. La Comisión Europea ha anunciado que el nuevo marco normativo tendrá la forma de un Reglamento y no de una Directiva, a diferencia de lo que se ha hecho en el pasado, y que traerá consigo cambios importantes dirigidos a dotar a las normas de una mayor aplicabilidad y adecuación frente a los cambios que tienen lugar en la sociedad de la información del siglo XXI.

El Reglamento que se propone adoptar, tendrá la ventaja, respecto a una directiva, de establecer un régimen armonizado que ofrezca un nivel homogéneo de protección en toda la UE. Una vez aprobado podrá aplicarse directa y universalmente en todos los Estados miembros de la UE, sin necesidad de una transposición a la legislación nacional.

Sin pretender entrar al detalle sobre las novedades de este nuevo marco normativo, dado que como es de esperarse es susceptible de ser modificado durante su proceso de adopción, pasaremos a destacar algunas de sus características.

Se opta por la aplicación de la normativa en función del lugar de residencia del titular de los datos. Es decir**,** cualquier compañía que trate datos personales en el contexto de las actividades de un establecimiento en un Estado miembro de la UE estará sujeta a estas nuevas regulaciones. La misma, se extiende a las organizaciones que se encuentran fuera de la UE pero que dirijan sus actividades de tratamiento de datos o monitoreo de comportamientos de individuos que residan en la UE.

Los principios universalmente aceptados de privacidad**,** calidad de los datos, transparencia en el tratamiento y proporcionalidad continuarán siendo medulares, agregándose otros, tales como la limitación al mínimo necesario de la recolección de datos personales, la rendición de cuentas (accountability) y la carga de la prueba en el responsable del tratamiento de datos personales.

Respecto al consentimiento del titular de los datos, éste continuará siendo una de las bases fundamentales de la normativa. Sin embargo, los requisitos para la obtención de un consentimiento válido e informado serán mucho más restrictivos. Se enfatiza la libertad del individuo para brindar o no sus datos personales, así como la obligación del contralor de los datos de probar la existencia del consentimiento.

También se proyecta la elaboración de una nueva directiva que regulará la protección de datos personales tratados con fines de prevención, detección, investigación y persecución de delitos y su respectiva actividad judicial.

Los Estados Unidos siguen un enfoque bipartito que permite por una parte la regulación de los datos personales recolectados por el sector privado, y por otra, los recolectados por el gobierno. Si bien el Privacy Act de 1974 permitió regular el almacenamiento de datos por parte del gobierno estadounidense, establecieron un sistema de auto-regulación para el sector privado (empresas privadas, actividades de búsqueda de datos, depósitos de datos personales, sitios de redes sociales e Internet, etc.). Fuera de unas pocas leyes que tratan de la información personal financiera y médica, Estados Unidos no cuenta con legislación que rija el procesamiento de datos personales por entidades privadas. En 1998 se implementó un sistema alternativo llamado "Safe Harbor" o "Puerto Seguro" para coordinar el intercambio de información con la Unión Europea.

Finalmente, varios países latinoamericanos basan su sistema en el Habeas Data, que es un derecho constitucional que permite al individuo conocer qué tipo de información personal se maneja por otros entes y el derecho que tiene de solicitar la supresión, rectificación, confidencialidad o actualización de cualquier dato. También le permite al individuo defender su honor, privacidad y honor. Varios países latinoamericanos han adoptado recientemente legislación amplia en esta materia.

Como veremos del cuadro contenido en la página 8, varios países han definido lo que es privacidad, varios otros contienen en sus constituciones la figura del Habeas Data, y otros más han adoptado legislación sobre la protección de datos.

A partir de la misma página 9 podemos encontrar un resumen de los esfuerzos que en las últimas décadas, algunas organizaciones internacionales han realizado para adoptar guías, principios, recomendaciones o instrumentos jurídicos en la materia.

Regresando al documento, a partir de la página 11 en adelante se hace una explicación de los regímenes en cada uno de los Estados miembros que respondieron al cuestionario del DDI, teniendo en cuenta el contenido particular de los mismos. La sección referida a cada país la hemos dividido en cuatro secciones. La primera se refiere a si el Estado de que se trata establece en su constitución el derecho a la intimidad, la figura de la protección de datos o el Habeas Data; analiza si el Estado en cuestión ha desarrollado legislación en esta materia; y establece si dichas normas se aplican al sector público o al sector privado. En la segunda sección se analiza si el Estado tiene alguna autoridad que implementa la legislación sobre la materia y analiza su relación con el gobierno; y determina los procedimientos a seguir en caso de que se produzcan violaciones a este derecho. También incluye información sobre el volumen y los tipos de quejas por parte de los individuos y determina si la autoridad responsable tiene o no capacidad de investigación y si dichas eventuales violaciones están sujetas a sanción penal. La tercera sección describe los posibles mecanismos existentes para la cooperación transfronteriza y establece si los Estados ponen límites o condiciones para transferir datos personales a otros países. Adicionalmente se incluye los acuerdos internacionales en los que se basa dicha cooperación y se determina los casos en que la ley permite que las autoridades pertinentes compartan información sobre los mecanismos de investigación con las autoridades de otras jurisdicciones. La cuarta parte analiza algunos casos que se han presentado en la práctica a nivel interno de los países.

Por las razones explicadas, la información contenida en el documento no refleja la situación de los países a esta fecha. Por ejemplo, la agencia de protección de datos de Costa Rica comenzó a funcionar posteriormente a la publicación del estudio y Colombia, promulgó la Ley Estatutaria No. 1581 del 17 de octubre de 2012 sobre protección de datos personales. Con el fin de mantener información completa y actual sobre la normativa de los países Miembros, el DDI ha creado la página web, que les mostraremos en unos momentos, y que entre otros aspectos contiene legislación actualizada no solo de los 11 países que respondieron el cuestionario sino de 17 Estados Miembros. Esta es una base de datos que está siendo perfeccionada y expandida.

Con toda esta información, creemos que las delegaciones tendrán suficientes elementos para poder discutir la necesidad de un marco regional en la materia. Creemos que, tal como lo hemos expresado en líneas anteriores, la importancia del tema es incuestionable, así como la necesidad de regularlo. El instrumento adecuado y las estrategias para llegar a dicho objetivo es lo que deberá ser determinado por el mejor saber y entender de los Estados miembros, ya sea a través de una declaración de principios, la elaboración de una Ley Modelo, la adopción de una Convención Interamericana, o la implementación de esfuerzos para intercambiar mejores prácticas y experiencias que lleven gradualmente a una harmonización de las leyes internas de los Estados miembros, para todo lo cual el Departamento de Derecho Internacional queda a su disposición.

Debemos tener en cuenta sin embargo, que no todo lo que parece pertenecer al ámbito de la protección de datos personales realmente lo es. No todo robo informático entra dentro de dicho ámbito. Por ejemplo, el robo de información de una base de datos militares que no contenga este tipo de información personal, no queda cubierto por este tema. Asimismo, el tele-mercado en sí mismo no queda cubierto por esta materia, ya que la empresa de tele-mercado bien podría haber obtenido el número de teléfono de una guía telefónica pública en la que el usuario registró su número por propia voluntad. Es en la manera cómo se obtuvo dicho dato donde radica el campo a ser regulado (por ejemplo, a través de redes sociales, o por obtención de la información a través de empresas que manejan información de tarjetas de crédito). Es importante pues tener muy en claro el campo al cual debe limitarse la regulación para que la norma sea clara, objetiva y útil al fin para el que fue creada.

Quiero finalizar recordando a las distinguidas delegaciones que otra herramienta que el DDI puso a su disposición fue el documento CP/CAJP-2921/10 rev.1 corr.1 “Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales de octubre de 2011, que contiene también elementos importantes para su consideración.

Muchas gracias,

Dante Negro
Director
Departamento de Derecho Internacional