CJI/doc.382/11

COMENTARIOS PRELIMINARES SOBRE UNA DECLARACIÓN DE PRINCIPIOS PARA LA PROTECCIÓN DE LA PRIVACIDAD Y DE LOS DATOS PERSONALES EN LAS AMÉRICAS

(presentado por el doctor David P. Stewart)

En su reciente 41ª. reunión en San Salvador, la Asamblea General de la OEA "encomendó al Comité Jurídico Interamericano que, antes del cuadragésimo segundo período ordinario de sesiones de la Asamblea General, presente un documento de principios de privacidad y protección de datos personales en las Américas … con miras a explorar la posibilidad de un marco regional en esta área". AG/RES. 2661 (XLI-O/11) (7 de junio de 2011). En este sentido, se instruyó al Comité Jurídico para que en la preparación del referido documento, se tuviese en cuenta (i) el Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales, que fuera preparado por el Departamento de Derecho Internacional (CP/CAJP-2921/10 rev. 1) y (ii) un estudio comparativo de diferentes regímenes legales, políticas y mecanismos de aplicación existentes para la protección de los datos personales que sería a su vez preparado por el Departamento de Derecho Internacional.

El Comité Jurídico Interamericano inicialmente consideró este tópico como parte de su tarea relativa al tema del "Acceso y Protección de la Información y de los Datos Personales en formato Electrónico", que había sido elaborado en respuesta a la directiva de la Asamblea General de la OEA según AG/RES. 2288 (XXXVII-O/07).[1] Al adoptar los Principios sobre el Derecho de Acceso a la Información,[2] no obstante, el Comité no enfocó específicamente los temas referidos al derecho a la privacidad y a la necesidad de proteger los datos personales. Ha llegado ahora el momento para que el Comité dirija su atención a estas importantes cuestiones.

Nadie niega la importancia de la protección de los datos personales en un mundo de rápida expansión de la tecnología de la información. El concepto de privacidad apuntala los principios fundamentales de la dignidad humana, así como la libertad de expresión, opinión y asociación. Estos principios están claramente establecidos en la Declaración Americana de los Derechos y Deberes del Hombre (1948)[3] así como en la Convención Americana de Derechos Humanos ("Pacto de San José").[4] Disposiciones similares se encuentran en la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y la Convención Europea de Derechos Humanos. Al mismo tiempo, resulta esencial proteger el libre flujo transfronterizo de informaciones. Ello, a su vez, protege y promueve la libertad de comercio, de la cual depende el avance económico y el desarrollo.

---

1 AG/RES. 2607 (XL-O/10) adoptando la Ley Modelo Interamericana sobre Acceso a la Información Pública, 8 de junio de 2010. Ver también AG/RES. 2514 (XXXIX-O/09), adoptada el 4 de junio de 2009.

2 Ver "Principios sobre el Derecho de Acceso a la Información," CJI/RES. 147 (LXXIII-O/08), adoptado el 7 de agosto de 2008.

3 La Declaración Americana de los Derechos y Deberes del Hombre dispone en el Art. IV que "toda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento, por cualquier medio" y en el Art. V que "toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honora, a su reputación, y su vida privada y familiar."

4 La Convención Americana de Derechos Humanos dispone en el Artículo 11 que: 1. Toda persona tiene derecho al respeto de su honora y al reconocimiento de su dignidad; 2. Nadie puede ser objeto de ingerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o su correspondencia, ni de ataques ilegales a su honra o reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas ingerencias o esos ataques. El artículo 13 de la Convención Americana de Derechos Humanos garantiza: 1. Toda persona tiene derecho a la libertad de pensamiento y expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideracion de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

Sin embargo, tal como lo reconocen todos los miembros del Comité Jurídico, las tecnologías de las comunicaciones globales y las prácticas mediáticas plantean serios y crecientes desafíos para las nociones fundamentales tales como privacidad, protección de datos y reputación, así como para la necesidad crucial de proteger y promover la libertad de expresión y de prensa y el libre flujo de información transfronteriza. La creciente sofisticación de la tecnología de la información digital permite a las entidades privadas, así como a los gobiernos, la posibilidad de recabar, analizar y diseminar mayor cantidad de información personal y más rápidamente que nunca. Por otro lado, los nuevos avances en lo que hace a la investigación y al cuidado médico, a las telecomunicaciones, a los sistemas de transporte avanzados y a las transferencias financieras han incrementado de manera dramática el nivel de información generado por cada individuo. Las computadoras en vinculadas entre sí mediante redes de alta velocidad con modernos sistemas procesadores pueden crear dossiers completos sobre cualquier persona en cualquier lugar, sin la necesidad de contar con un sistema de computación central.

Las aplicaciones involucrando estas tecnologías nuevas incluyen a las tarjetas de identidad, a la biométrica (por ejemplo fotografías digitalizadas, escáner de retina, geometría manual, reconocimiento de la voz, identificación por DNA, vigilancia de las comunicaciones, intercepción de la internet y de los correos electrónicos, vigilancia por video (televisión en circuito cerrado) y así sucesivamente. Estas tecnologías están disponibles de manera creciente, no solamente para los gobiernos, sino también para el sector privado, incluyendo las compañías comerciales, los periodistas y los miembros de los medios, e incluso para grupos de defensa no comerciales. Numerosas aplicaciones son totalmente legítimas y legales. Por ejemplo, las empresas comerciales recogen, almacenan y diseminan información personal sobre clientes y consumidores; algunas, de manera rutinaria, recaban información a partir del uso del correo electrónico y de la internet para fines de mercadeo. Lamentablemente, no es poco común ver que se utilizan para fines impropios o incluso ilícitos, como por ejemplo el monitoreo no autorizado de las comunicaciones, las actividades y la localización de personas públicas y privadas, de los oponentes políticos, de los trabajadores que militan en el área de los derechos humanos, periodistas y organizadores laborales, y competidores económicos.

Hoy en día, una mayoría de países reconoce el derecho a la privacidad de manera explícita en sus constituciones. Como mínimo, estas disposiciones incluyen los derechos de la inviolabilidad de domicilio y de la confidencialidad en las comunicaciones. Muchas constituciones nacionales, (tal como las de Sudáfrica y Hungría) garantizan derechos específicos de acceso y control de la propia información personal. En muchos otros países donde la privacidad no se encuentra explícitamente reconocida en la constitución nacional (tal como en los Estados Unidos, Irlanda e India) los tribunales han encontrado dicho derecho en varias disposiciones legislativas. En otros, los acuerdos internacionales que reconocen los derechos de privacidad han sido adoptados e implementados por la legislación.

En todo el mundo, un movimiento general está presionando para la adopción de legislación específica sobre privacidad doméstica que establezca marcos legales nacionales para la protección de los datos individuales. Dentro de la OEA, el esfuerzo está comenzando a conseguir su *momentum.* Hasta la fecha, unos pocos estados (incluyendo, por ejemplo, México, Perú, Costa Rica, Canadá y Brasil) han adoptado recientemente, o están trabajando de manera activa sobre nueva legislación en el área de la privacidad. No obstante, no existe ningún modelo regional o abordaje coordinado para tratar sobre estos temas en el ámbito nacional. Tampoco la Corte Interamericana de Derechos Humanos ni la Comisión Interamericana de Derechos Humanos parece otorgar atención significativa a estos temas.[5]

---

[5] Ver el Informe de la Comisión sobre terrorismo y Derechos Humanos (párrafos 280-95 discutiendo el *habeas data*). Ver también el reciente Informe del relator Especial de la ONU sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión (Frank La Rue), doc. ONU A/HRC/17/27 (mayo 16, 2011), en párrafo 59 ("existen leyes sobre la protección de datos insuficientes o inadecuadas en muchos Estados que estipulan quién puede acceder a los datos personales, para qué pueden ser utilizados, cómo deben ser almacenados, y durante cuánto tiempo.")

Así las cosas, el Comité tiene la oportunidad de brindar una contribución significativa en este campo. Al hacerlo de esta manera, podría por supuesto tener en cuenta los esfuerzos que han sido desplegados en otras regiones, así como los amplios estudios sobre privacidad de datos que se están llevando a cabo en la Organización para la Cooperación y el Desarrollo Económico, en Europa (en el Consejo de Europa así como en la Unión Europea), en el Foro Económico de Asia-Pacífico, y en otros lugares.

OCDE. En 1980, la Organización para la Cooperación y el Desarrollo Económico adoptó principios no vinculantes y tecnológicamente neutros para su uso posible en el establecimiento, sea de un marco legal o un estándar industrial. Las ocho "Directrices que Rigen la Protección de la Privacidad y de los Flujos de Datos Personales Transfronterizos" se aplican tanto a los usos de los datos personales en el ámbito gubernamental como en el privado. Ellos requieren 1) limitar la captura de datos personales y asegurar que dicha información pueda solamente obtenerse por medios legítimos y justos y, cuando apropiado, mediando el conocimiento o el consentimiento del titular de los datos; 2) asegurar que la información recogida sea importante para los fines para los cuales será utilizada, debiendo también ser precisa, complete actualizada; 3) especificar las finalidades para las cuales se recogen los datos personales; 4) no divulgación ni uso de los datos para fines diferentes de aquellos especificados con anterioridad; 5) proteger los datos mediante salvaguardias que otorguen razonable seguridad; 6) establecer una política general de abertura sobre avances, prácticas y políticas relacionadas con los datos personales; 7) brindar a los individuos el derecho de obtener datos personales dentro de un plazo de tiempo razonable y también de manera razonable; y 8) responsabilizar a los controladores de datos por el cumplimiento de los requerimientos contenidos en estos principios.

Europa. El enfoque de los países europeos con relación a los temas de privacidad y de protección de los datos se ha basado en gran medida en una combinación de leyes nacionales, de la Convención de 1981 del Consejo de Europa para la Protección de Individuos con Respecto al Procesamiento Automatizado de Datos Personales (ETS Nº. 108), la Convención Europea de 1950 sobre Derechos Humanos y Libertades Fundamentales y la Carta de Derechos Fundamentales de la Unión Europea de 2007, con más una serie de directivas y reglamentaciones de la UE.

La propia UE adoptó primeramente una regla sobre protección de datos en 1995, requiriendo a cada Estado miembro de la UE que adoptase legislación adecuada a dicha regla.[6] En ese momento, la Directiva sobre Datos de la UE podía solamente regir para el sector privado, porque las facultades de la UE eran limitadas (previo al Tratado de Lisboa). Desde ese entonces ha sido complementado por una Directiva sobre Privacidad Electrónica de la UE.[7] Hablando en términos generales, estas directivas requieren que los datos sean procesados de manera justa y legal, debiendo ser capturados para fines específicos y legítimos, ser adecuados y ajustados a dichas finalidades, además de precisos y actualizados, no pudiendo ser retenidos más allá de lo necesario. Por otro lado, una Directiva sobre Telecomunicaciones establece hoy en día protecciones específicas en lo que hace a sistemas telefónicos, de televisión digital, de redes de celulares y de otros sistemas de telecomunicaciones.[8] La Directiva sobre Telecomunicaciones impone obligaciones de gran escala sobre los operadores (o portadores) y los proveedores de servicio, a fin de asegurar la privacidad de las comunicaciones de los usuarios. El acceso a los datos de

---

[6] Directiva 95/46, oct. 24, 1995) sobre la protección de los individuos con relación al procesamiento de los datos personales, modificada por la Directiva 2002/22/EC sobre servicio universal y derechos de los usuarios referidos a las redes de comunicación electrónicas y sobre el libre movimiento de tales datos.

[7] Directiva 2002/58 (julio 12, 2002), modificada en 2006 y más recientemente por la Directiva 2009/136 (nov. 25, 2009) y servicios. Ver también Directiva 2002/58/EC, relativa al procesamiento de datos personales y la protección de la privacidad en el sector de comunicaciones electrónicas, y la Reglamentación (EC) Nº 2006/2004 sobre cooperación entre las autoridades nacionales responsables por el cumplimiento de las leyes de protección al consumidor.

[8] Directiva 2006/24 (marzo 15, 2006) sobre la retención de los datos generados o procesados en conexión con el suministro de servicios de comunicación electrónica públicamente disponibles o de redes de comunicaciones públicas. Otros instrumentos europeos relevantes incluyen la Convención de 1981 del Consejo de Europa para la Protección de los Individuos con Relación al Procesamiento Automático de los Datos Personales (ETS Nº 108).

facturación será severamente restringido, así como las actividades de mercadeo. La tecnología del identificador de llamadas deberá incorporar una opción el bloqueo de la transmisión de número de línea. La información recogida al entablarse una comunicación debe destruirse una vez completada la llamada.

Todos los países de la UE poseen un "inspector de privacidad" o agencia que vela por la observancia de las reglas,[9] y se espera que los países extranjeros con los cuales los miembros de la UE hacen negocio adopten un nivel de inspección que se ajuste a dichas normas. En otras palabras, las Directivas apuntan a garantizar que los derechos de los sujetos europeos con relación a sus datos continúen protegidos. Así, las Directivas prohíben la exportación de datos a países fuera de la UE que carecen de un "nivel adecuado" de protección de datos conforme determinado por la Comisión Europea. Como resultado, no se permite a las compañías que operan dentro de la UE enviar datos personas a países fuera de la UE, a menos que dichos países puedan garantizar que los datos recibirán niveles de protección equivalente a los requisitos establecidos en la UE. Estas restricciones ejercen presión sobre otros países para que se adecuen a los estándares europeos. Los países (y las compañías) que se niegan a adoptar leyes significativas sobre privacidad podrán encontrar que no pueden realizar ciertos tipos de flujos de información con Europa, particularmente cuando dicha información involucra datos sensibles.

Estados Unidos. En los Estados Unidos, la Constitución Federal ha sido interpretada a fin de incluir un derecho a la privacidad,[10] y varias reglamentaciones federales sobre privacidad abordan la protección de los datos y temas referidos a la misma en contextos o sectores de actividad específicos, tal como los informes sobre créditos (Ley Federal de Informes sobre Créditos de 1970), datos sobre salud (Ley de 1996 de Responsabilidad y Portabilidad de la Información sobre Salud) la captura por parte del gobierno federal de datos personales (Ley de Privacidad de 1974, la Ley de Gobierno Electrónico de 2002, la Ley de Confidencialidad Impositiva), etc. Otras áreas de actividad comercial están activamente regladas en el ámbito estatal (y a veces local). No toda la actividad del sector privado está necesariamente sujeta a la reglamentación sobre privacidad, y a diferencia de la UE y de sus estados miembros, no existe ninguna legislación ómnibus o de finalidad genérica referida a la protección de los datos. Sin embargo, se está considerando de manera activa la consideración de nueva legislación tanto a nivel federal (esta primavera, los senadores Kerry y McCain presentaron la Declaración de Derechos sobre Privacidad Comercial de 2011) así como en varios estados (incluyendo Vermont, Massachusetts, Illinois, y California).

La diferencia entre el enfoque de los Estados Unidos respecto de la privacidad comercial y la directiva de 1995 de la UE sobre Protección de Datos fue vinculada por medio del marco denominado de "puerto seguro (protección legal)" adoptado por los Estados Unidos y la UE conjuntamente a fines de la década de 1990. El marco de Puerto Seguro es un innovador arreglo transnacional diseñado para preservar el libre flujo de información y comercio. Permite a ciertas compañías de los Estados Unidos autocertificarse de que siguen los Principios de Privacidad del Puerto Seguro, cumpliendo así con los estándares sobre reglamentaciones de la privacidad en la UE. Como resultado de ello, la UE permitirá la transferencia de datos personales a los receptores que hayan adherido a los principios del Puerto Seguro y que se encuentren sujetos a las autoridades de aplicación de la comisión de Comercio federal de los Estados Unidos o al Departamento de Transporte de los EE.UU.

Los principios del Puerto Seguro requieren que las compañías brinden siete garantías en particular: (1) aviso – los individuos deben estar informados de que sus datos están siendo capturados y la manera en que van a ser utilizados; (2) elección – los individuos deben tener la posibilidad de excluir la captura y transferencia de sus datos a terceros; (3) "transferencia ulterior" – las transferencias de datos a terceros solamente pueden tener lugar para organizaciones que

---

[9] Ver, por ej., Reglamentación (EC/CE) Nº 1211/2009 del Parlamento Europeo y del Consejo del 25 de noviembre, 2009, estableciendo el Cuerpo de Reguladores Europeos para Comunicaciones electrónicas (BEREC por sus siglas en inglés).

[10] Entre las decisiones importantes se encuentran Olmstead c/ Estados Unidos, 277 U.S. 438 (1928) (voto en disenso del Juez Brandeis); Griswold c/ Connecticut, 381 U.S. 479 (1965); y Loving c/ Virginia, 388 U.S. 1 (1967).

siguen los principios de protección de datos adecuados; (4) seguridad – se deben desplegar esfuerzos razonables para prevenir la pérdida de la información recogida o capturada; (5) "integridad de los datos" – los datos deben ser relevantes y confiables para los fines para los cuales fueron capturados; (6) acceso – Los individuos deben tener la posibilidad de contar con acceso a la información que se tenga sobre ellos mismos, y corregirla o eliminarla cuando sea inexacta; y (7) cumplimiento (observancia) – deben existir medios efectivos de hacer cumplir estas reglas. Las organizaciones que adopten estos principios deben re-certificar su cumplimiento cada 12 meses, sea por medio de una autoverificación o mediante la realizada por tercero(s). Debe también proveerse capacitación apropiada de los empleados y mecanismos de solución de controversias.

APEC. Por otro lado, se está siguiendo un enfoque diferente en los países de la Cuenca del Pacífico dentro del foro de Cooperación Económica Asia-Pacífico (APEC), la cual, más que buscar la armonización de leyes internas sobre privacidad, enfocó de manera más específica el tema de las transferencias transfronterizas de datos personales. Durante varios años la APEC ha estado trabajando en una iniciativa sobre privacidad. En 2004 se adoptó un Marco con Principios sobre Privacidad, agregándose un programa de implementación en 2005, a fin de estimular la implementación doméstica en los estados miembros con relación a los Principios. Por otro lado, un subgrupo ha estado trabajando sobre Privacidad de Datos a fin de desarrollar reglas de privacidad Transfronterizas (CBPR por sus siglas en inglés), permitiendo la certificación de los negocios para transferencia de información personal entre las economías que participan de la APEC. Además, en 2010 se estableció un Acuerdo de Cooperación para la Observancia de la Privacidad Transfronteriza (CPEA, siglas en inglés) con el fin de brindar reconocimiento mutuo entre las economías que participan de la APEC sobre los mecanismos de cada parte para la certificación de las reglas de privacidad de los negocios (La OCDE posee una red similar de aplicación llamada GPEN.)

Existe una cierta dosis de coincidencia en los principios adoptados por estos varios grupos. Como mínimo, todos requieren que la información personal debe ser obtenida limpiamente y de conformidad con la ley; debe ser utilizada de manera compatible con la finalidad originalmente especificada, debe ser precisa y actualizada; de distribución limitada para terceros; y destruida luego de haberse satisfecho su finalidad. Al mismo tiempo, existen también algunas diferencias significativas en el enfoque, incluyendo si en todo caso - y cuándo y cómo - se deben aplicar los mismos principios para las entidades gubernamentales, proveedores de servicios públicos, empresas comerciales privadas, e incluso individuos; y temas de aplicación del derecho penal y seguridad nacional, en oposición a las organizaciones.

El documento preparado por el Departamento de Derecho Internacional (CP/CAJP-2921/10 rev. 1) establece una serie de principios preliminares bastante detallados titulados: Legitimidad y justicia; Propósito específico; Limitados y necesarios; Transparencia; Rendición de cuentas; Condiciones para el procesamiento de datos; Transferencias internacionales; Derecho de la persona al acceso a la información; Derecho a la persona a corregir y suprimir sus datos personales; derecho a objetar el procesamiento de datos personales; Legitimación para ejercer los derechos sobre el procesamiento de los datos personales; Medidas de seguridad para proteger los datos personales; Deber de confidencialidad, y Control, cumplimiento y responsabilidad.

La labor del Comité será revisar estas propuestas cuidadosamente, a la luz de los esfuerzos de otros grupos y entidades, y con la atención puesta en la específica cultura legal y en las necesidades de los miembros de la OEA y de su región. Entre las cuestiones a ser consideradas se encuentra el alcance de la aplicación (las partes privadas así como los órganos gubernamentales), el efecto sobre la seguridad nacional y los intereses en la aplicación de la ley, el requisito (más que la opción) de contar con una autoridad central supervisora, el impacto sobre las leyes y prácticas existentes (y en preparación) en el ámbito nacional, la relación de principios restrictivos sobre el flujo transfronterizo de información y sobre el libre comercio, y la necesidad de excepciones o derogaciones conforme sea apropiado para las circunstancias.

La amenaza a la privacidad es ahora mayor que en cualquier momento de la historia reciente. El poder, capacidad y velocidad de la tecnología de la información están acelerando rápidamente, y con ellos la amplitud de la invasión en la privacidad. La globalización ha removido las limitaciones geográficas para el flujo de datos. Existe la necesidad de principios claros y efectivos para brindar

protección adecuada a la privacidad sin entorpecer indebidamente otros intereses importantes. Esa es la tarea para la cual se ha solicitado ahora la participación del Comité.

REFERENCIAS

KNIGHT, S. “Regulatory Conflict over Data Privacy: Can the US-EU Safe Harbor Arrangement Be Sustained?” (American Consortium on European Union Studies, 2003).

SHAFFER, G. “Extraterritoriality in a Globalizing World: Regulation of Date Privacy,” 97 Am. J. Int’l L. 314, 2003.

KENYON, A. and RICHARDSON, M. (eds.). New Dimensions in Privacy Law: International and Comparative Perspectives. Cambridge, 2006

LEVMORE, S. and NUSSBAUM, M. (eds.). The Offensive Internet: Privacy, Speech and Reputation. Harvard, 2010

NOORDA, C. and HANLOSER, S. (eds.). E-Discovery and Data Privacy: A Practical Guide. Kluwer, 2011.