CJI/doc.402/12 rev. 2

PROPUESTA DE DECLARACIÓN DE PRINCIPIOS DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES EN LAS AMÉRICAS

(presentada por el doctor David P. Stewart)

En su cuadragésimo primer período ordinario de sesiones, en San Salvador en 2011, la Asamblea General de la OEA le encomendó al Comité Jurídico Interamericano que presentara "antes del cuadragésimo segundo período ordinario de sesiones de la Asamblea General, 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).

Para la elaboración de estos principios, se instruyó al Comité que tomara en cuenta (i) el Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales preparado por el Departamento de Derecho Internacional (CP/CAJP-2921/10 rev. 1) y (ii) un estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, que elaborará el Departamento de Derecho Internacional.

En su 79º período ordinario de sesiones, en agosto de 2011, el Comité consideró por primera vez esta labor, con base en los Comentarios Preliminares que figuran en el documento CJI/doc.382/11 (del 18 de marzo de 2011). El Comité también nombró a un Relator para que preparara un conjunto de principios propuestos en respuesta al mandato de la Asamblea General.

A su vez, el Departamento de Derecho Internacional presentó el documento que contiene los "Principios y Recomendaciones Preliminares sobre la Protección de Datos (la Protección de Datos Personales)," CP/CAJP-2921/10 rev. 1 corr. 1, del 11 de octubre de 2011. El 31 de octubre de 2011, el Departamento distribuyó entre todos los Estados miembros de la OEA un cuestionario sobre privacidad y protección de datos, con miras a determinar el estado actual de la evolución y las propuestas legislativas en este ámbito (CP/CAJP-3026/11). Más recientemente, el Departamento distribuyó un "bosquejo anotado" largo y detallado de su "Estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación para la protección de datos personales" (DDI/doc.03/12, del 10 de febrero de 2012).

No cabe duda que el concepto de la privacidad está firmemente establecido en el derecho internacional y que sostiene los principios fundamentales del honor y la dignidad personal, así como de la libertad de expresión, opinión y asociación. En nuestro hemisferio, estos principios están establecidos claramente en la Declaración

Americana de los Derechos y Deberes del Hombre (1948)[1] así como en la Convención Americana sobre Derechos Humanos ("Pacto de San José").[2] En todos los sistemas de derechos humanos más importantes del mundo figuran disposiciones sobre la privacidad, la protección del honor y de la dignidad de la persona, la libertad de expresión y de asociación y el libre flujo de información.[3]

Estos principios fundamentales se han visto crecientemente desafiados por la revolución en las tecnologías digitales de la información y las comunicaciones. Hoy en día vivimos en una "economía global de la información". Se obtiene, procesa y publica más información sobre las personas más rápidamente que en cualquier otro tiempo, tanto por gobiernos como por entidades privadas, incluyendo empresas comerciales, periodistas y otros comunicadores sociales, e incluso por grupos de presión no empresariales. Ante estas circunstancias, es más importante que nunca tomar medidas para proteger los derechos fundamentales de las personas a la privacidad. Por otro lado, es necesario reconocer que la recopilación de datos personales e información de y sobre individuos con frecuencia no sólo es apropiada, sino necesaria, y que muchas aplicaciones son enteramente legítimas y legales. También es esencial reconocer que en una economía que se está globalizando a gran velocidad, el flujo irrestricto de información entre fronteras sigue siendo un requisito para una economía libre y dinámica; las limitaciones innecesarias pueden imponer barreras no arancelarias significativas (y a menudo no intencionales) al comercio y al desarrollo. Aunque es cierto que ocurren abusos y que es necesario abordarlos, las reglas excesivas y las disposiciones demasiado restrictivas pueden causar más daño que bien.

En todo el mundo, las autoridades nacionales se están esforzando para abordar estos temas, y, lo que no es sorprendente, en ocasiones adoptan enfoques distintos y aplican valores opuestos de maneras incongruentes. En la actualidad, la mayoría de los países reconocen el derecho constitucional a la privacidad y muchos otros ofrecen protecciones adicionales de la privacidad mediante leyes o normas, entre las que se incluyen particularmente las que imponen restricciones al gobierno y a las instituciones públicas. Más de 80 países ya tienen leyes sobre protección de datos y

---

[1] Véase el art. IV de la Declaración Americana de los Derechos y Deberes del Hombre.

[2] Véanse los arts. 11 y 13 de la Convención Americana sobre Derechos Humanos.

[3] Véanse, por ejemplo, la Declaración Universal de los Derechos Humanos (arts. 12, 18-20), el Pacto International de Derechos Civiles y Políticos (arts. 17-19), el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (arts. 8-10), la Carta de los Derechos Fundamentales de la Unión Europea (arts. 1, 7, 8, 10-12) y la Carta Africana de Derechos Humanos y de los Pueblos (arts. 5, 8-11 y 28). Solamente la Carta de la UE aborda específicamente la privacidad en el contexto de la protección de datos. El art. 8 estipula que (1) toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan, (2) estos datos se trataran de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley y toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación y (3) el respeto de estas normas quedará sujeto al control de una autoridad independiente.

privacidad que van más allá del sector público, y en muchos otros se están llevando a cabo actividades legislativas.[4] Sin embargo, las disposiciones específicas de ninguna manera son idénticas. El resultado es una diversidad de leyes, normas y reglas nacionales que reflejan distintos enfoques en muchos aspectos importantes.[5]

Además, en los últimos decenios se han emprendido intensos esfuerzos para adoptar principios acordados a nivel regional e internacional, en particular dentro de la Organización para la Cooperación y Desarrollo Económicos (OCDE), el Consejo de Europa, la Unión Europea (UE) y el foro de Cooperación Económica Asia Pacífico (APEC).[6] Los más significativos de estos esfuerzos se resumieron en el informe anterior al Comité (en CJI/doc.382/11 del 18 de marzo de 2011). Pero los documentos adoptados por estos distintos organismos de ninguna manera son idénticos; difieren tanto en sus detalles como en su enfoque fundamental.

Al analizar estos diversos enfoques nacionales y regionales se detectan ciertos rasgos en común como divergencias significativas en principio y en enfoque. Por ejemplo, no parece haber una definición única y comúnmente aceptada de información "personal" o "sensible" o "protección de datos", y mucho menos de la "privacidad" en sí. Tampoco existe un concepto único y acordado de "amenaza" o de la respuesta apropiada a tal amenaza. Hay quienes consideran la recopilación y el uso de información privada por parte del gobierno y de sus agencias como la principal amenaza y se proponen restringirlas, mientras que otros temen más al sector privado y buscan protección en la supervisión y reglamentación por parte del gobierno.

Algunos desean empoderar a las personas, en especial a los consumidores, poniendo énfasis en el consentimiento, la transparencia, "responsabilidad" de las empresas, y la "gestión de los datos", mientras que otros prefieren que el gobierno

---

[4] México, Uruguay, Perú, Colombia, Costa Rica, Canadá y Brasil, entre otros.

[5] Como se indica en el documento CP/CAJP-2921/10 rev. 1 corr. 1, "el significado de la privacidad y los orígenes del derecho individual a la privacidad pueden variar. En consecuencia, las políticas y leyes que rigen el derecho a la privacidad difieren de un país a otro. Habida cuenta de esta divergencia en el tratamiento del derecho a la privacidad, la legislación que protege el tratamiento de los datos personales puede variar de una región a otra e incluso dentro de una misma región".

[6] La UE sustituirá en fecha próxima el esquema establecido en la Directiva 95/46 (del 24 de octubre de 1995) sobre la protección de las personas en lo relativo al procesamiento de los datos personales, de acuerdo con el cual han venido operando durante trece años tanto los sectores público como privado en los países miembros. Las enmiendas que se anunciaron el 25 de enero de 2012 (que entrarán en vigor después de algunos años) prometen un nuevo "Reglamento" para la UE dirigido a integrar un "mercado digital único" que reemplazará a los distintos enfoques nacionales hacia la aplicación de la Directiva anterior. El nuevo Reglamento consagrará el "derecho de ser olvidado", que ha sido sujeto de considerables debates. Dentro del Consejo de Europa, la Gran Sala del Tribunal Europeo de Derechos Humanos expidió recientemente un fallo significativo en torno a la privacidad en *Axel Springer vs. Alemania*, App. No. 39954/08 (7 de febrero de 2012), en el que mantuvo que se habían violado los derechos del editor del tabloide alemán *Bild* según el art. 10 cuando se le impidió publicar artículos sobre el arresto y la condena por posesión de cocaína de un actor de televisión bien conocido.

reglamente a todos los "recopiladores, administradores y controladores de los datos". Algunos intentan abordar estas cuestiones a través de una sola ley integral, mientras que otros adoptan un enfoque sectorial o temático, con distintos niveles de supervisión gubernamental para los diferentes tipos de actividades, de maneras distintas. Algunos defienden el "derecho de ser olvidado" (que incluye un derecho a la eliminación de toda la información, incluso si es veraz), mientras que otros proponen un derecho a la "rectificación" o a la "corrección" (en el sentido de un derecho a que se corrijan errores e inexactitudes).

Es evidente que el tema es dinámico, la discusión se mantiene activa, y los enfoques tanto nacionales como regionales siguen evolucionando. Cuáles prácticas específicas son aceptables y cuáles se deben circunscribir o prohibir muy probablemente dependerá de la manera en que se aborde el problema. Las respuestas pueden diferir si se consideran desde la perspectiva de la seguridad nacional o de la aplicación de las leyes, o como asunto de reglamentación social, o desde la perspectiva de proteger la innovación tecnológica, promover el comercio y el desarrollo, proteger contra intrusiones del extranjero, etc. Por el momento es necesario concluir que no existe una "talla única". Un intento de describir o imponer un solo enfoque normativo detallado tiene pocas probabilidades de lograr aprobación amplia a corto plazo.

Lo que tiene más probabilidad de aceptación, y lo que parece haber solicitado la Asamblea General de la OEA, es una declaración de principios generales para orientar la consideración futura de estas cuestiones. Los siguientes principios (adjuntos como Anexo A) se han formulado con vistas a cumplir ese objetivo y a partir de un análisis de las legislaciones y prácticas nacionales emergentes, así como de los principios acordados (aunque divergentes) de los distintos grupos regionales e internacionales que hasta ahora han abordado el problema.

Además del Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales que elaboró el Departamento de Derecho Internacional (CP/CAJP-2921/10 rev. 1 corr. 1) y del "bosquejo anotado" de su "Estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales" (DDI/doc.03/12), el Relator consideró las siguientes fuentes internacionales para la preparación de estos principios propuestos:

- Los Principios de Privacidad de la APEC, adoptados como parte del Marco de Privacidad de la APEC y de su Sistema de Reglas de Privacidad Transfronteriza de 2011.
  http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx, y
  http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf

- Las directrices de la OCDE sobre la protección de la privacidad y flujos transfronterizos de datos personales de 1980.
  http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
- El Convenio del Consejo de Europa para la protección de las personas contra el procesamiento automático de datos personales, de 1981.
  http://conventions.coe.int/treaty/en/treaties/html/108.htm
- La Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Diario Oficial N° L 281 del 23 de noviembre de 1995 p. 0031 - 0050.
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT
- Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), Bruselas, 25.1.2012, COM (2012) 11 final, 2012/0011 (COD).
  http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales de las Naciones Unidas, adoptados por medio de la Resolución 45/95 de la Asamblea General de la ONU (14 de diciembre de 1990).
  http://www.un.org/documents/ga/res/45/a45r095.htm

Aunque los principios adjuntos se inspiran en buena parte en estas esfuerzos anteriores (así como en una variedad de legislaciones nacionales), se han orientado intencionalmente a contener un nivel de generalidad que permita su aceptación en sistemas jurídicos nacionales que se encuentran en distintas etapas de consideración del tema y que pueden tener distintas orientaciones y prioridades. También reflejan el hecho de que la OEA, como organización regional, difiere en muchos aspectos de la Unión Europea y del Consejo de Europa, así como de la APEC y la OCDE. Los principios propuestos están encaminados a establecer parámetros básicos ampliamente aceptables para su desarrollo ulterior, y no a imponer un modelo o enfoque particular para su implementación directa en todos los Estados miembros de la OEA.

Anexo A

PROPUESTA DE DECLARACIÓN DE PRINCIPIOS DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES EN LAS AMÉRICAS

Introducción

La siguiente lista establece los principios básicos que deberían adoptarse y aplicarse en las leyes y prácticas nacionales. La intención de estos es evitar daños a las personas derivados de la obtención o uso incorrecto o innecesario de datos personales e información personal. Los doce principios están interrelacionados y deben interpretarse como un conjunto global. Además, cada sistema nacional debería adoptar una política clara y eficaz de apertura y transparencia con respecto a todos los sucesos, prácticas y políticas relacionados con los datos personales y la información personal. En razón de lo anterior, el Comité Jurídico Interamericano propone a la Asamblea General de la OEA la adopción de los siguientes principios:

Principio Uno: Propósitos Legítimos y Justos

Los datos personales y la información personal deben ser recopilados solamente para fines legítimos y por medios justos y legales.

Principio Dos: Claridad y Consentimiento

Se deben especificar los fines para los cuales se recopilan los datos personales y la información personal en el momento en que se recopilen. Como regla general, los datos personales y la información personal solamente deben ser recopiladas con el conocimiento o el consentimiento de la persona a que se refieran.

Principio Tres: Pertinencia y Necesidad

Los datos y la información deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación.

Principio Cuatro: Uso Limitado y Retención

Los datos personales y la información personal deben ser mantenidos y utilizados solamente de manera legítima no incompatible con el fin o fines para los cuales se recopilaron. No deberán mantenerse más del tiempo necesario para su propósito o propósitos y de conformidad con la legislación nacional correspondiente.

Principio Cinco: Deber de Confidencialidad

Los datos personales y la información personal no deben divulgarse, ponerse a disposición de terceros ni emplearse para otros propósitos que no sean aquellos para los cuales se obtuvieron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley.

Principio Seis: Protección y Seguridad

Los datos personales y la información personal deben ser protegidos mediante salvaguardias razonables y adecuadas contra accesos no autorizados, pérdida, destrucción, uso, modificación o divulgación.

Principio Siete: Fidelidad de la Información

Los datos personales y la información personal deben mantenerse fieles y actualizados hasta donde sea necesario para los propósitos de su uso.

Principio Ocho: Acceso y Corrección

Se debe disponer de métodos razonables para permitir que aquellas personas, cuya información ha sido recopilada, puedan solicitar el acceso a dicha información y puedan solicitar a la persona encargada de su manejo que la modifique, corrija o elimine. En caso de que fuera necesario restringir dicho acceso o corrección, deberían especificarse las razones concretas de cualquiera de estas restricciones de acuerdo con la legislación nacional.

Principio Nueve: Información Sensible

Algunos tipos de información, teniendo en cuenta su sensibilidad y en contextos particulares, son especialmente susceptibles de causar daños materiales a las personas si se hace mal uso de ellos. Las personas o entidades encargadas de la información deberían adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los individuos sujetos de la información.

Principio Diez: Responsabilidad

Las personas o entidades encargadas de la información adoptarán las medidas correspondientes para el cumplimiento de estos principios.

Principio Once: Flujo Transfronterizo de Información y Responsabilidad

Los Estados miembros cooperarán entre sí en la creación de mecanismos y procedimientos que aseguren que aquellas personas o entidades encargadas de la información que operen en más de una jurisdicción puedan ser efectivamente hechas responsables por el cumplimiento de estos principios.

Principio Doce: Publicidad de las Excepciones

Cuando las autoridades nacionales establezcan excepciones a estos principios por motivos relacionados con la soberanía nacional, la seguridad interna o externa, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, deberían poner en conocimiento del público dichas excepciones.

* * *