ANEXO XX

PRINCIPIOS Y RECOMENDACIONES PRELIMINARES SOBRE LA PROTECCIÓN DE DATOS

(LA PROTECCIÓN DE DATOS PERSONALES)

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS 17 octubre 2011
COMISIÓN DE ASUNTOS JURÍDICOS Y POLÍTICOS Original: inglés

-- Índice de contenido --

PRINCIPIOS Y RECOMENDACIONES PRELIMINARES SOBRE LA PROTECCIÓN DE DATOS

(LA PROTECCIÓN DE DATOS PERSONALES)

I. INTRODUCCIÓN

Antecedentes de procedimientos

Desde 1996, la Asamblea General de la Organización de los Estados Americanos (OEA) viene dedicando especial atención a las cuestiones vinculadas al acceso a la información y a la protección de los datos personales y, por resolución AG/RES. 1395 (XXVI-O/96), solicitó al Comité Jurídico Interamericano (CJI) que iniciara un estudio de los contextos jurídicos de los Estados Miembros de la OEA en relación con estos dos temas. Sobre el tema "acceso a la información pública", la Asamblea General solicitó una labor adicional a los Estados Miembros y a los órganos, organismos y entidades de la OEA por vía de las resoluciones siguientes: AG/RES. 2057 (XXXIVO/ 04), AG/RES. 2121 (XXXV-O/05), AG/RES. 2252 (XXXVI-O/06), AG/RES. 2288 (XXXVIIO/ 07), AG/RES. 2418 (XXXVIII-O/08) y AG/RES. 2514 (XXXIX-O/09). Esta labor culminó con la aprobación de la resolución AG/RES. 2607 (XL-O/10), en junio de 2010, que incluye el texto de una "Ley modelo interamericana sobre acceso a la información pública" y en la que también se encomendaba a la Secretaría General que brindara apoyo a los Estados Miembros en el diseño, ejecución y evaluación de sus contextos jurídicos locales en relación con el acceso a la información pública.

Sobre el tema de la protección de los datos personales, la Asamblea General solicitó varios estudios y documentos al Comité Jurídico Interamericano sobre el acceso/protección de la información y los datos personales, como OEA/Ser.Q CJI/doc. 52/98, CJI/doc.25/00 rev.1, CJI/doc.162/04, CJI/doc.232/06 rev.1, CJI/doc.25/00 rev.2 de 2007 y CJI/doc.239/07. El Comité Jurídico Interamericano aprobó también resoluciones sobre la materia, como las resoluciones CJI/RES.9/LV/99, CJI/RES.33 (LIX-O/01), CJI/RES.81 (LXV-O/04) y CJI/RES.130 (LXXI-O/07), todo ello, en un

empeño por abordar la regulación de la protección de datos a través de posibles instrumentos internacionales y a nivel de la legislación de algunos Estados miembros de la OEA, así como a nivel del tratamiento de datos personales por el sector privado. Estos trabajos aportaron elementos valiosos, no sólo para comprender la verdadera dimensión de esta cuestión a la luz de los efectos de las nuevas tecnologías en la expansión del manejo y el uso de la información por los particulares, sino también para ayudar a los Estados a adoptar medidas en cuanto a la armonización de las legislaciones, el fomento de la cooperación regional y la búsqueda de elementos sustanciales para un futuro instrumento regional sobre la materia.

Además de la labor del Comité Jurídico Interamericano, la Asamblea General solicitó que la Secretaría General preparase el presente estudio preliminar sobre la protección de datos con la finalidad de ofrecer una perspectiva general de los temas más relevantes a considerar en la elaboración de los principios y recomendaciones sobre la protección de datos [AG/RES. 2288 (XXXVII-O/07), AG/RES. 2418 (XXXVIII-O/08), AG/RES. 2514 (XXXIX-O/09) y AG/RES. 2661 (XLI-O/11), "Acceso a la información pública y protección de datos personales"]. El proyecto de un estudio preliminar fue enviado a los Estados Miembros el 19 de noviembre de 2010 (CP/CAJP-2921/10). Posteriormente, el 13 de diciembre de 2010, la Comisión de Asuntos Jurídicos y Políticos (CAJP) del Consejo Permanente sostuvo una sesión especial sobre el tema "acceso a la información pública". En esa ocasión, la Presidencia de la CAJP solicito a las delegaciones presentar sus comentarios al proyecto de estudio, los cuales se incluyen en la versión revisada. Mediante la nota CP/CAJP-2932/11, fechada el 28 de enero de 2011, la Presidencia formalizó esta petición.

Antecedentes sustantivos

El CJI explicó en su Informe Anual a la Asamblea General de 2007 que los avances en la tecnología de la computación y la Internet, así como en medicina y biotecnología dieron lugar a un marcado incremento en el tratamiento de datos personales en las diversas esferas de la actividad económica y social. Los avances logrados en la tecnología de la información – que han dado lugar a notables beneficios sociales y económicos – tornan relativamente fácil y, a menudo, necesarios el procesamiento e intercambio de datos entre países. Por tanto, el desafío es proteger los derechos y libertades fundamentales, en especial el derecho a la privacidad y el derecho al acceso a información personal (también conocido como habeas data) y, al mismo tiempo, estimular el flujo libre y seguro de información dentro y fuera de un país, lo cual es esencial para la continua expansión del comercio electrónico, computación en nube y otros servicios web.

A este respecto, es ampliamente reconocido que el uso de sistemas electrónicos para el procesamiento, recolección, almacenamiento, transferencia y divulgación de información personal crece exponencialmente cada año. En consecuencia, la cantidad y los tipos de información personal disponible sobre las personas es causa de preocupación de algunos defensores de la privacidad. Y, aunque es difícil determinar qué datos personales están (privada o públicamente) disponibles – un problema que se complica por la amplia gama de actores estatales y no estatales custodios de la información personal – muchos promueven nuevos métodos para regular cómo se recaba la información y cómo se emplea. La industria –en particular los generadores de tecnología – han hecho también un llamamiento a la reforma Estos llamamientos con frecuencia se centran en el desnivel entre la tecnología y la regulación, ya que aquélla ha evolucionado a gran velocidad, en tanto ésta lo ha hecho a un ritmo mucho más lento. Los regímenes regulatorios anticuados pueden obstaculizar la innovación y dejar a los consumidores sin la suficiente protección. Por esta razón, es de suma importancia que los Estados Miembros de la OEA unan esfuerzos para promover un marco armonizado y duradero para la protección de datos.

La legislación sobre la protección de datos se basa en el derecho de las personas a la privacidad. Sin embargo, 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. En términos generales, el tratamiento de la protección de datos ha seguido uno de tres criterios. El europeo es hoy el sistema más estricto de regulaciones estatales, con una legislación que rige la recolección de datos personales por parte del gobierno y las entidades privadas. El sistema de Estados Unidos sigue un criterio bifurcado, que permite que los sectores económicos regulen los datos personales recabados por organizaciones privadas y la regulación estatal de los datos recabados por el Estado. Por último, varios países de América Latina han elaborado mecanismos de protección de datos basados en el concepto de habeas data, el cual es un derecho constitucional que permite a las personas acceder a sus propios datos personales y otorga el derecho a corregir toda información errónea.

Varios países latinoamericanos han tomado medidas para regular la protección de datos en el ámbito nacional. México, por ejemplo, recientemente llevó a cabo una reforma integral que pretende combinar los diversos criterios. La nueva Ley federal para la protección de datos personales, apro-

bada en julio de 2010 y que entra en vigor en enero de 2012, combina algunos aspectos de autorregulación con la capacidad de corregir los datos erróneos y una supervisión legal.

En Colombia, el Congreso de la República aprobó el 16 de diciembre de 2010 la nueva ley sobre protección de datos personales. Esta ley regula de manera integral el derecho constitucional que tienen todos los colombianos a conocer, actualizar y rectificar la información que sobre ellos se haya recogido en bases de datos o archivos. Esta ley que sigue los estándares internacionales sobre la materia (resolución 45/95 de las Naciones Unidas, Convenio 108 de Consejo de Europa, Directiva Europea 95/46 y Resolución de Madrid de 2009) incorpora por primera vez en la región elementos novedosos en el tratamiento de datos personales como lo son las Normas Corporativas Vinculantes (BCR) y procesos de autorregulación empresarial para un desarrollo más efectivo de la protección de datos Entre otros países que recientemente adoptaron leyes sobre protección de datos en la región se incluye Argentina, Perú y Uruguay. Como se detallará más adelante, pese a estos enfoques diferentes en la regulación de los datos personales, existen algunos principios fundamentales que han servido de base para la legislación sobre la protección de los datos en todo el mundo.

Teniendo en cuenta la marcada diferencia en el tratamiento del derecho a la privacidad y la protección de los datos entre Europa, Estados Unidos y Canadá, en la parte primera del presente trabajo se ofrece un breve panorama sobre el derecho a la privacidad y la protección de los datos en estas jurisdicciones. En la parte segunda se examinará el habeas data y su incidencia en la protección de los datos personales. La parte tercera ofrece un análisis de las definiciones que resultan fundamentales para la protección de los datos personales y, en la cuarta, se detallarán, pues, los 15 principios que son la base de la legislación sobre protección de datos en todo el mundo y que podrían servir de base para un instrumento internacional o una legislación modelo sobre la protección de datos. Cada sección fundamental incluirá también recomendaciones correspondientes a cada uno de los principios. La parte quinta de este documento concluye con medidas proactivas que los Estados Miembros de la OEA podrían adoptar para proteger los datos personales y fomentar la cooperación entre las autoridades nacionales e internacionales.

II. LA PROTECCIÓN DE DATOS EN EUROPA, ESTADOS UNIDOS Y CANADÁ

El Consejo de Europa reconoce el derecho a la privacidad como un "derecho humano fundamental"(1) .Además, la Declaración Universal de Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos definen a la privacidad como un derecho "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación."(2) Los dos tratados explican luego: "Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"(3). En consecuencia, la visión europea del derecho a la privacidad cubre todos los aspectos de la vida del individuo. En base a esta perspectiva expansiva del derecho a la privacidad, la legislación europea correspondiente cubre el procesamiento de datos personales por organizaciones gubernamentales y privadas (4). El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal ("el Convenio") define en términos generales los datos personales como "toda información relacionada con una persona identificada o identificable" y describe los principios de la protección de datos, que han servicio de base para la legislación en este campo en todo el mundo (5). Más tarde, en la Directiva sobre protección de datos de la Unión Europea ("la Directiva") se afirmó que los principios sobre protección de datos consagrados en los consiguientes principios del Convenio fijaban el nivel estándar de la protección de datos para los miembros de la Unión Europea y, aún más importante, reconoció el derecho de los particulares a la privacidad (6). A raíz de esta preocupación expansiva por el derecho a la privacidad del individuo, la Directiva pasa a admitir la transferencia de datos personales a países de fuera de la Unión Europea sólo cuando el país afectado "garantice un nivel de protección adecuado [de los datos]" o si demuestra que los datos quedarán debidamente protegidos una vez que hayan sido transferidos (7). De esta manera, la Directiva amplía a los países fuera de sus fronteras el alcance de la protección otorgada a los datos personales originados en la Unión Europea.

El alcance de la Directiva se ha extendido más allá de las fronteras europeas, y ha incidido en la regulación de la protección de datos en todo el mundo, al obligar a otros países con empresas interesadas en transferir datos personales a examinar su propia legislación sobre protección de datos y, de ser necesario, modificarla para satisfacer los estándares de la Unión Europea (8). Cabe destacar, sin embargo, que la Comisión Europea emprendió una re-

visión de la Directiva en 2010 debido, en parte, a que "es preciso mejorar, en general, los mecanismos existentes de transferencia internacional de datos personales". El Vicepresidente de la Comisión Europea responsable de la Agenda Digital ha explicado también que el marco regulatorio relativo a la protección de datos de la Unión Europea debe ser actualizado conforme a la era digital a fin de proteger los derechos fundamentales y, al mismo tiempo, "tener la mejor economía y mejores condiciones de vida que permiten las tecnologías digitales". Se anticipa que hacia finales de año se presente una propuesta para una nueva ley que reemplace a la Directiva.

En Estados Unidos, los orígenes del derecho a la privacidad pueden encontrarse en su Constitución y en el derecho consuetudinario (9). En uno de los artículos más influyentes de ese país sobre el derecho a la privacidad, los autores argumentaban que el de la privacidad era el "derecho a que a uno lo dejen tranquilo" (10). Desde entonces, la Suprema Corte de Estados Unidos se ha pronunciado en favor de los intereses privados derivando el derecho a la privacidad de la Constitución (11). En sus decisiones, la Suprema Corte ha declarado que la Constitución protege el interés de las personas de evitar la divulgación de sus asuntos personales y el interés en la independencia para tomar cierto tipo de decisiones importantes (12). Sin embargo, la Suprema Corte también ha sostenido que el derecho a la privacidad no era absoluto y que el interés de una persona por su privacidad debe ponderarse frente a la competencia del interés público (13).

En Estados Unidos, el derecho a la privacidad, a diferencia del enfoque europeo, protege sólo contra la intrusión del gobierno federal en los asuntos privados de las personas. Por ende, la legislación específica sobre la cuestión de la protección de los datos personales se limita a los datos tratados o custodiados por el gobierno federal (14). Fuera de unas pocas leyes que tratan de la información personal financiera y médica, Estados Unidos no cuenta con una legislación que rija el procesamiento de datos personales por entidades privadas (15). Por el contrario, el sistema de ese país prevé la auto regulación por parte de los sectores económicos en materia de datos personales manejados por entidades privadas. En tal sentido, los sectores de la actividad privada de Estados Unidos están básicamente autorregulados, incluida la mayoría de las empresas privadas, las actividades de búsqueda de datos, los depósitos de datos personales y los sitios de redes sociales de Internet, entre otros. Sin embargo, debe tenerse en mente que también existen muchas leyes en materia de privacidad de aplicación estatal. Durante el último año, la Comisión Federal de Comercio y el Departamento de Comercio de Estados Unidos han publicado proyectos de informes y recomendaciones para lograr que la privacidad sea protegida de manera más amplia y en todo el

país. En tales proyectos han dejado en claro que el objetivo de asegurar que el creciente y cambiante mercado de la información tenga sus bases en la promoción de la privacidad, la transparencia, la innovación empresarial y las opciones para el consumidor (16). Asimismo, el Congreso de ese país ha tomado en consideración varias propuestas relativas a la privacidad.

En los casos en que quieran cumplir con directrices predeterminadas sobre el manejo de datos personales, los particulares pueden ampararse en una disposición de la Comisión Federal de Comercio de Estados Unidos por la que certifica que la entidad en cuestión establece un nivel adecuado de protección de los datos personales.17 Aunque esta disposición tiene carácter voluntario en el contexto interno, las empresas que reciben datos personales de miembros de la Unión Europea deben emplear estas pautas para el manejo de información transfronteriza. Además, el hecho de que la legislación estadounidense se centre exclusivamente en la protección de la información de las personas que procesa el gobierno federal, no queda claro cuál es el nivel de protección asignado a los datos personales procesados por entidades privadas en Estados Unidos y, luego, transferidos a otro país (18).

En Canadá, la privacidad es protegida gracias a un régimen legislativo de varios niveles. Las actividades de las instituciones gubernamentales en relación con los datos personales están sujetos a la Carta de Derechos y Libertades de Canadá, que forma parte de la Constitución. A este respecto, el Tribunal Supremo de Canadá ha reconocido que el derecho a oponerse a un registro e incautación, mencionado en la sección 8 de la Carta, protege contra toda injerencia injustificada por parte del Gobierno en la privacidad que razonablemente espera tener un individuo. Aunque esta disposición no es una prohibición absoluta a la injerencia del Estado en la privacidad de una persona, sí permite asegurar que cualquier actividad del Gobierno en este sentido sólo represente una interferencia razonable. El Gobierno federal y todas las provincias y territorios también tienen leyes que rigen la recolección, uso, divulgación y eliminación de la información personal en manos de entidades gubernamentales.

Con respecto a la protección de datos en el sector privado, Canadá se adhirió a las Directrices de la OCDE en 1984 y promovió la autorregulación, como ocurrió en Estados Unidos. En el año 2000, el Parlamento de Canadá aprobó una ley de aplicación general en toda la nación para la protección de información personal. En dicha ley se estableció un conjunto de normas que han de aplicarse uniformemente en el mercado canadiense, de modo que existan garantías tanto para los consumidores como para las empresas y se fomente la confianza en el comercio electrónico. Esta ley se ajusta a las leyes sobre la privacidad en el sector privado, en el ámbito subnacional en cuanto que

son "sustancialmente similares" a la ley federal. Algunas provincias han promulgado leyes que son también aplicables a las actividades no comerciales del sector privado.

III. PROTECCIÓN DE DATOS EN AMÉRICA LATINA

Habeas data

Literalmente, habeas data significa "debes tener los datos"(19). Aunque sus orígenes pueden encontrarse en Europa, el habeas data en América Latina es una acción que se entabla ante la justicia para permitir la protección de la imagen, la privacidad, el honor, la determinación por sí misma de la información y la libertad de información de una persona (20). El habeas data es un mecanismo que otorga a la persona la facultad de detener el abuso de sus datos personales (21). En general, permite a la persona el acceso a la información personal en las bases de datos públicas o privadas, la capacidad de corregir y actualizar los datos y la posibilidad de asegurarse de que los datos delicados mantengan su confidencialidad, y permite el retiro de los datos personales delicados que pueden atentar contra el derecho a la privacidad (22). A diferencia de las leyes de protección de datos de Europa y Estados Unidos, el habeas data no exige que las entidades públicas y privadas protejan por su iniciativa los datos personales que procesan, sino que sólo requiere que la persona agraviada, tras presentar una denuncia ante la justicia, obtenga acceso y la capacidad de rectificar todo dato personal que pueda atentar contra su derecho a la privacidad (23). Además, el habeas data se reserva como recurso legal sólo para personas a las que se compromete su privacidad (24) Además, este mecanismo puede no otorgar un recurso legal a una persona agraviada si sus datos personales han sido transferidos fuera del país (25). En consecuencia, la protección del habeas data es más limitada que la del modelo europeo. Algunos países, como Argentina, por ejemplo, han aprobado leyes de protección de los datos personales que complementan la legislación ya vigente de habeas data (26).

Legislación reciente

México aprobó una nueva Ley federal sobre la protección de los datos personales, en julio de 2010. A diferencia del criterio de Estados Unidos, que principalmente regula el procesamiento de datos por entidades del Estado, la nueva ley mexicana regula el tratamiento de datos personales exclusivamente por el sector privado. Además, el Instituto Federal de Acceso a la Información, que antes de la aprobación de la nueva Ley sobre Datos Personales ejercía la supervisión exclusiva del acceso a información en custodia de organismos estatales, ahora posee facultades ampliadas para incluir la

supervisión del sector privado en lo que hace a los datos personales, aunque la nueva ley, paradójicamente, no se aplica a los datos personales procesados por organismos estatales. Aunque existen interrogantes en relación con el funcionamiento de la nueva ley mexicana, marca una evolución importante en la legislación sobre protección de la privacidad y de los datos en las Américas y, junto con los regímenes de la Unión Europea, Estados Unidos y del habeas data, ofrece una serie de principios y normas que ayudan a regular esta importante esfera dentro de los Estados Miembros de la OEA.

Colombia aprobó en 2010 una nueva ley general de protección de datos, la cual incorpora los principales lineamientos internacionales sobre la materia al igual que elementos innovadores como el de la autorregulación. La nueva ley se encuentra actualmente en revisión por parte de la Corte Constitucional y se espera que el fallo correspondiente se emita en junio de 2011. La ley aprobada por el Congreso regula de manera integral el derecho que tienen todos los Titulares a conocer, actualizar y rectificar la información que sobre ellos repose en bases de datos o archivos. Las disposiciones contenidas en esta ley son aplicables para bases de datos tanto de naturaleza pública como privada, estableciendo así, bajo una sola normatividad las obligaciones de Responsable y Encargados tanto del sector público como privado.

IV. DEFINICIONES

A los efectos del presente documento, es importante definir claramente los conceptos básicos que se relacionan con la protección de datos personales puesto que las definiciones podrían más tarde afectar otros aspectos, como quién tiene derecho a presentar una denuncia alegando la violación de las leyes de protección de datos ante la justicia y el alcance de las leyes de protección de datos. Al mismo tiempo, cabe hacer hincapié en la necesidad de mantener la flexibilidad en las definiciones dado que el método exacto para alcanzar los objetivos de un sistema de protección de datos debe garantizar la flexibilidad como medio para reflejar el hecho de que los países del Hemisferio han adoptado diferentes perspectivas con respecto a la protección de datos. Los siguientes son algunos de los conceptos cuyas definiciones deben ser tomadas en cuenta.

Datos Personales

El Convenio y las Directrices sobre protección de la privacidad y flujos fronterizos de datos personales de la Organización para la Cooperación y el Desarrollo Económicos ("las Directrices") definen en general los "datos personales" como "toda información relacionada con una persona identificada o identificable." (27). Por ende, las Directrices y el Convenio podrían

aplicarse a los datos personales de personas naturales y jurídicas. Algunos países, en reconocimiento de la ambigüedad, trataron de formular definiciones más claras. Por ejemplo, la Resolución de Madrid dice que "datos personales" significa "cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados"(28). Por tanto, la Resolución de Madrid amplió su protección a todos los datos personales que puedan vincularse a una persona. Por otro lado, la Ley de protección de datos de Argentina define los datos personales como "información personal de cualquier tipo referida a personas o entidades jurídicas determinadas o determinables"(29). La legislación de Argentina ofrece protección de los datos personales de las entidades públicas y privadas. No obstante, la Ley de protección de datos del Reino Unido, por ejemplo, establece explícitamente que los "datos personales son datos que se relacionan con una persona viva que pueda ser definida" (30). Por su propia definición, la Ley del Reino Unido no comprende a las personas fallecidas. Sin embargo, si quedan en la ambigüedad, las leyes de protección de datos podrían extenderse a los datos de las personas después de su muerte. Debe entenderse, por lo tanto, que la definición de datos personales afectará los datos del individuo cuya información se protege, y que dicho individuo podría más adelante alegar violaciones a la protección de datos, y con ello posiblemente se limite el período de protección de los datos.

Controlador de datos y procesador de datos

Las Directrices definen en términos generales al "controlador de los datos" como "la persona natural o jurídica, la autoridad pública, el organismo o cualquier otra entidad competente de acuerdo con la legislación nacional para decidir el propósito de un archivo de datos automatizado" (31). El Convenio también define en general al "controlador de datos" en el sentido de que incluye a "una parte que, de acuerdo con la legislación nacional, es competente para decidir…el uso de los datos personales".32 En consecuencia, las Directrices y el Convenio se aplican tanto a entidades públicas como privadas que tratan de los datos personales. Sin embargo, en Australia y Canadá, que tienen una legislación separada para los datos procesados por el Estado y los datos procesados por organizaciones privadas, claramente definen al controlador de datos como dependiente de la legislación.33 Además, el Reino Unido y España establecen una diferenciación entre el "controlador de datos" y el "procesador de datos"34 En el Reino Unido y en España, el procesador de datos procesa los datos en nombre del controlador de datos.35 En efecto, el procesador de datos actúa como agente en nombre del controlador de datos.36 Por esa razón, el controlador de datos sigue siendo responsable de asegurar que todos los datos personales procesados por un

procesador de datos en su nombre cumplan con la ley (37). El "controlador de datos", por oposición al simple "procesador de datos", debe estar claramente definido porque esta definición determinará, en última instancia, quién es responsable de cumplir con las leyes de protección de datos.

La Resolución de Madrid de 2009, que se constituye en el primer esfuerzo para establecer estándares internacionales sobre esta materia incorpora los términos de Responsable del Tratamiento de datos, que es la Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos o el tratamiento de los datos.

Datos personales sensibles

El Reino Unido y España se cuentan entre los países cuyas leyes de protección de datos definen los "datos personales sensibles" en el sentido de que consisten en información sobre origen racial o étnico, opiniones políticas, religión, actividades sindicales, salud física o mental, preferencias sexuales y antecedentes penales.38 La categoría de datos que se consideran sensibles debe estar claramente definida, porque los datos sensibles pueden requerir un tratamiento especial, como el consentimiento explícito para su divulgación o, tal vez, la existencia de una prohibición contra el procesamiento de este tipo de datos, a menos que exista una excepción en la ley. Al mismo tiempo, es importante reconocer que otros sistemas legislativos no definen datos confidenciales. La legislación canadiense, provincial y federal, sobre la protección de datos, por ejemplo, no suele incluir una definición de datos confidenciales debido a que estas leyes no establecen categorías de tipos de datos de carácter personal ni reconocen que la determinación de la confidencialidad puede depender en gran medida del contexto de que se trate.

Procesamiento

El Convenio define el "procesamiento automático" como el almacenamiento, la realización de operaciones lógicas y/o aritméticas…la alteración, supresión, recuperación o divulgación.39 El Reino Unido eliminó el adjetivo "automático" de su definición y define el "procesamiento" describiendo prácticamente todo uso imaginable de datos por un controlador de datos.40 La Resolución de Madrid opta por una definición muy amplia pero ambigua del procesamiento y comprende todo uso posible de los datos personales.41 Dicha Resolución también dispone que la misma se aplica a "cualquier procesamiento de datos personales, total o parcialmente por medios automáticos o, por lo demás, en forma estructurada, y realizado en el sector público o en el sector privado".42 Australia no emplea la palabra "procesamiento", optando en su lugar por "uso" (43). Australia define el "uso" como el manejo de información personal dentro de una organización.44 El procesamiento de datos debe ser definido ampliamente y, tal vez,

en esta instancia, pueda ser útil dejar la definición ambigua para asegurar que la mayor diversidad posible de usos de los datos personales, incluida su recolección, esté protegida por la ley.

Sin embargo, como en la Resolución de Madrid, podría ser necesario limitar la definición del procesamiento de datos, a fin de excluir el "procesamiento de datos personales por personas naturales… relacionadas exclusivamente con su vida privada y familiar", a fin de dejar en claro que la legislación sobre protección de datos no tiene el objetivo de ser aplicada a personas que podrían procesar datos personales en el curso de sus actividades privadas.45 También podría ser necesario exceptuar del cumplimiento de la legislación sobre protección de datos personales a los organismos encargados de hacer cumplir la ley, actuando bajo su autoridad legítima y en circunstancias muy limitadas, conforme lo autorice la legislación interna (46).

Consentimiento

La persona afectada debe consentir debidamente el procesamiento de sus datos personales. La definición del consentimiento, sin embargo, debe ser lo suficientemente flexible como para permitir que las leyes nacionales enuncien explícitamente cuándo se requiere el consentimiento y qué tipo de consentimiento se requiere en diferentes circunstancias. Por lo general, el consentimiento dado por el individuo debe ser definido como una "manifestación libre, específica y fundada" del acuerdo de una persona con respecto al tratamiento de datos personales (47). Sin embargo, al definir el consentimiento, no se debe inferir necesariamente que la falta de respuesta al pedido de un controlador de datos para procesar los datos personales constituye un consentimiento de la persona afectada (48) Más bien es importante tomar en cuenta el contexto a fin de determinar qué tipo de consentimiento es adecuado, incluso si el procesador pretende tratar los datos sólo conforme a las prácticas comúnmente aceptadas. Además, es importante tomar nota de que puede haber circunstancias, en particular en lo que respecta al tratamiento de datos personales por parte de organismos públicos (es decir, organismos encargados del cumplimiento de las leyes), donde no debe requerirse el consentimiento.

Siempre que sea aplicable, la definición del consentimiento debería incluir la posibilidad de retirar dicho consentimiento, limitar el período de validez del mismo49 o, en determinadas circunstancias, requerir que el consentimiento sea renovado para usos diferentes de los que la persona pudo haber previsto. En términos más generales, el controlador de datos debe brindar a la persona procedimientos sencillos para retirar rápida y totalmente el consentimiento (50). Además, la determinación de la validez o no del consentimiento podría depender de la edad, capacidad mental y

circunstancias imperantes en el momento de expresarse al controlador de datos para procesar los datos personales (51). Es posible que se requiera el consentimiento de terceros, como un padre o tutor, cuando la persona no sea capaz de indicar debidamente el consentimiento (52). El consentimiento adecuado puede ser implícito o explícito. Sin embargo, cuando se trate de datos personales sumamente sensibles, el consentimiento debe ser explícito.53 Ello significa que la persona debe indicar inequívocamente su acuerdo con el procesamiento de sus datos personales (54).

V. PRINCIPIOS Y RECOMENDACIONES

Los principios que se enumeran a continuación han servido de base para la legislación sobre protección de datos. Los principios, algunos de los cuales están interrelacionados, incluyen también recomendaciones jurídicas, que explican cada uno de ellos. Es importante señalar, sin embargo, que los principios pretenden centrarse en los objetivos que deben lograrse en términos generales, en lugar de describir en detalle lo que deben contener las leyes nacionales.

Principio 1: legitimidad y justicia

Los datos personales deben ser procesados legítima y justamente. Sin embargo, la legitimidad y la justicia, como conceptos, deben examinarse por separado.

Legitimidad

El procesamiento de los datos personales debe ser legítimo. Si el procesamiento de datos personales comporta cometer un delito penal o contraviene un deber impuesto por la ley, entonces puede ser ilegítimo.55 Por ejemplo, el procesamiento ilegal de datos también podría implicar el incumplimiento de un deber, como lo son la confianza, una obligación contractual o la legislación internacional de derechos humanos (56).

Justicia

El procesamiento de datos personales debe ser justo. La Resolución de Madrid establece que "todo procesamiento de datos personales que da lugar... a discriminación" contra la persona es injusto (57). Para que el procesamiento de datos sea justo debe mediar una razón legítima para "recabar y usar los datos personales" (58). El procesamiento de datos personales no debe tener "efectos adversos injustificados para la persona afectada" (59). El procesamiento de datos personales debe ser transparente. Un proceso transparente incluye notificar al interesado quién está procesando sus datos personales,

si los datos serán compartidos con otros y el uso que se pretende dar a los datos (60). Asimismo, con unas cuantas excepciones, los datos personales deben ser procesados sólo en la forma que la persona afectada "puede razonablemente prever".61 Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, podría existir un uso injusto de los datos personales. A esa altura, podría corresponder procurar el consentimiento de la persona para seguir procesando sus datos personales (62).

Principio 2: propósito específico

Los datos personales deben ser procesados con un "propósito específico, explícito y legítimo" (63). Ello significa que, desde el comienzo, el propósito del procesamiento de los datos personales debe ser inequívoco (64). Ello también significa que el propósito del procesamiento de datos personales debe ser acorde a las expectativas razonables de la persona afectada en el momento en que se obtuvo u otorgó el consentimiento (65). Asimismo, si se están procesando datos personales sensibles, debe requerirse el consentimiento explícito de la persona (66). Si se proyecta procesar los datos personales con un propósito incompatible con los propósitos para los que fueron obtenidos, se necesita el consentimiento inequívoco de la persona afectada (67). Para determinar si un nuevo propósito o divulgación es compatible con el propósito original para el cual se obtuvieron los datos, podría ser necesario determinar si el nuevo uso proyectado de los datos personales es justo y legítimo (68). En su defecto, podría ser necesario determinar si el nuevo propósito surgió del contexto del propósito original para percibir si existe relación entre el nuevo propósito y el propósito primario (69). Además, si se trata de datos personales sensibles, el nuevo propósito debe "relacionarse directamente" con el propósito primario o lo que constituya una práctica comúnmente aceptada (70). Los principios y recomendaciones, sin embargo, deben ser lo suficientemente flexibles como para permitir que en las leyes nacionales se indique explícitamente cuándo se requiere el consentimiento y qué tipo de consentimiento se requiere en diferentes circunstancias.

Principio 3: limitados y necesarios

Los datos personales que se procesen deben limitarse a los necesarios para un propósito específico.

Limitados

El procesamiento de datos personales debe ser limitado. Eso significa que el procesamiento debe ser adecuado, relevante y no excesivo en rela-

ción con los propósitos para los cuales se recabaron los datos personales (71). Asimismo, el procesamiento de datos personales debe limitarse a la razón del momento para procesarlos (72). Ello significa que debe procesarse sólo la cantidad mínima de datos personales para cumplir debidamente el propósito de que se trate (73). Sin embargo, la cantidad de datos personales debe bastar para cumplir el propósito específico para el cual se obtuvieron y procesaron los datos (74). Asimismo, los datos personales no deben divulgarse, otorgarse o de alguna otra manera usarse para otros propósitos que no sean los específicos para los que originalmente se recabaron y procesaron, excepto medie el consentimiento de la persona afectada o decisión de la autoridad legítima (75).

Necesario

Debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario (76). Si se requieren los datos personales para la consecución efectiva de una función o actividad legítima, el procesamiento de datos personales será necesario (77). Más específicamente, el procesamiento de datos personales sólo será necesario si el mismo "contribuye directamente" a la consecución del objetivo para el cual fueron obtenidos y procesados los datos (78). Si el objetivo puede lograrse por otros medios razonables, no es necesario el procesamiento de datos personales (79). A continuación se indican algunas condiciones que hacen necesario el procesamiento de datos personales: 1) la concertación o ejecución de un contrato; 2) el cumplimiento de una obligación legal; 3) la protección de los intereses de la persona; 4) la satisfacción del interés de justicia, y 5) la protección de los legítimos intereses del controlador de datos, a menos que ello perjudique o dañe los intereses de la persona afectada.80 Además, aunque no debe admitirse el procesamiento de datos personales que "pueden ser útiles en el futuro", podría ser necesario procesar datos personales "para una posibilidad previsible que puede nunca materializarse" (81).

Principio 4: transparencia

Es importante que el procesamiento de datos personales sea transparente. La transparencia en el procesamiento de datos personales es especialmente importante si la persona tiene la opción de establecer o no una relación con el controlador de datos (82). A continuación se indican algunos elementos que pueden contribuir a asegurar la transparencia en el procesamiento de datos personales.

Información sobre el controlador de datos

Cuando procese datos personales, el controlador de datos debe ofrecer, como mínimo, la información siguiente a la persona afectada: 1) información sobre la identidad del controlador de datos; 2) el propósito del procesamiento de los datos personales; 3) las personas o categorías de los proveedores de servicio a quienes se podrán revelar los datos personales; 4) la forma en que la persona afectada puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos, y 5) toda otra información necesaria para el justo procesamiento de los datos personales (83). Cuando sea posible, el controlador de datos debe hacer lo que sea necesario para orientar a las personas sobre la situación específica en que se divulgarán sus datos; asimismo, deberá indicar cuál es la entidad que autoriza al controlador de datos a procesar los datos personales (84).

Dado que en el futuro podría afectar aspectos de jurisdicción o elección del derecho aplicable, es importante incluir la identidad del representante local del controlador de datos, si éste se encuentra en un tercer país (85). Cuando divulgar información sobre el controlador de datos. Si los datos personales fueran recabados directamente de la persona, la información sobre el controlador de datos y sobre el propósito del procesamiento de datos debe brindarse en el momento de la recolección, si ya no se brindó la información (86). Si los datos personales de la persona afectada se obtuvieron de un tercero, el controlador de datos debe informar a la persona afectada de la fuente de los datos personales (87) La información debe brindarse "dentro de un plazo razonable". Sin embargo, si ello es impracticable o implica un esfuerzo desproporcionado de parte del controlador de datos, podrían usarse otros métodos para informar a la persona (88) Cómo divulgar información que implica el procesamiento de datos personales La información debe brindarse a la persona en forma "inteligible, empleando un lenguaje claro y sencillo" (89) Toda la información debe ser descodificada y, de ser necesario, debe incluir explicaciones (90). La información debe ser comprendida por una persona promedio (91). Tal vez sea necesario traducir la información a otro idioma o tener en cuenta necesidades especiales de los menores, cuando se proporcione información sobre el procesamiento de datos personales (92).

Jurisdicción y ley aplicable

Aquellos controladores que operen en varios mercados pueden experimentar ciertos desafíos por lo que toca a la transparencia, en particular en cuanto a la identificación de leyes y autoridades que rigen el procesamiento de los datos personales de una persona, en el entendido de que sólo pueden aplicarse las leyes de un Estado Miembro. Podría ser difícil, por ejemplo, determinar la jurisdicción y ley aplicable (incluidas las obligaciones en materia de transparencia) en casos en que se cree, procese y almacene un sólo conjunto de datos, y al que

se tenga acceso en varios países. Los Estados pueden mejorar la transparencia en el procesamiento de datos proporcionando reglas predecibles y claras para determinar cuál régimen nacional prevalecerá sobre ciertos datos.

Principio 5: rendición de cuentas

El controlador de datos es responsable de adoptar todas las medidas necesarias para seguir las pautas del procesamiento de datos personales que imponga la legislación nacional u otra autoridad competente (93). Además, recae en el controlador de datos la responsabilidad de demostrar a las personas y a la autoridad supervisora pertinente que cumple con las directivas necesarias, conforme lo establezca la legislación nacional u otra autoridad, para proteger los datos personales de quien se trate.94 Esto último debe incluir cómo gestiona el controlador de datos los pedidos de acceso a información sobre datos personales y qué tipo de información personal procesa (95).

En resumen, la ley debe responsabilizar a todas las organizaciones por la forma en que se procesen los datos que les han sido encomendados. En un marco de responsabilización, las normas y requerimientos para la protección de datos están consagradas en las leyes, y cada una de las organizaciones debe determinar cómo han de acatar tales normas en la práctica. Asimismo, la ley debe reconocer que las medidas que se hayan de tomar para implementar estos elementos deben ser "escalables", es decir, que deben depender de la naturaleza y volumen de la información personal que se procese, la naturaleza de dicho procesamiento y los riesgos para los individuos afectados.

Principio 6: condiciones para el procesamiento de datos

El procesamiento de datos personales sólo debe mediar si se da alguna de las condiciones siguientes y si el procesamiento es justo y legítimo (96).

Consentimiento

El controlador de datos debe obtener el consentimiento libre, inequívoco e informado de la persona, antes de procesar sus datos personales.97 Como ya se explicó, puede ser necesario obtener el consentimiento de un tercero, si la persona afectada es incapaz de brindar un consentimiento adecuado. Asimismo, es posible que sea necesario el consentimiento explícito para procesar información sensible. La definición del consentimiento, sin embargo, debe ser lo suficientemente flexible como para permitir que en las leyes nacionales se indique cuándo y qué tipo de consentimiento se requiere.

Interés legítimo del controlador

El interés legítimo del controlador podría justificar el procesamiento de los datos personales de un individuo (98). Sin embargo, deben ponderarse los intereses y derechos legítimos de la persona afectada contra los intereses del controlador de datos (99). Si prevalecen los intereses de la persona, no se deben procesar sus datos (100). Debe plantearse la necesidad de que existan disposiciones legales que permitan al controlador realizar el procesamiento o tratamiento.

Obligaciones contractuales

De ser necesario, puede admitirse el procesamiento de los datos personales antes o durante la ejecución de una relación contractual entre el controlador de datos y la persona afectada (101). Ello debe incluir el procesamiento necesario para propósitos operativos vinculados al cumplimiento de un contrato, como puede ser el procesamiento con propósitos contables y de facturación, monitoreo, apoyo y mejoramiento de servicios y validación de los sujetos.

Deben existir las garantías suficientes para que en caso de violación a los datos existan mecanismos compensatorios y efectivos en las relaciones contractuales.

Autoridad legal

Se admite el procesamiento de los datos personales de un individuo si ello es necesario para que el controlador de datos cumpla un deber impuesto por una autoridad del Estado (nacional o extranjero) o si dicho procesamiento es realizado por el controlador de datos, siendo una entidad pública, en ejercicio legítimo de su autoridad (102). Esta condición también rige para los órganos encargados de hacer cumplir la ley que procesan datos personales en el curso de sus deberes de investigación, autorizados por la legislación nacional (103).

Circunstancias excepcionales

Se admite el procesamiento de datos de una persona si ello es necesario para evitar o atenuar un perjuicio inminente y grave para su vida, salud o seguridad o para la vida, salud o seguridad de otra persona (104). El controlador de datos debe estar razonablemente convencido de que el procesamiento de esos datos personales es necesario para evitar el daño (105). No se debe recurrir como rutina a esta condición para procesar datos personales (106). Además, las amenazas a la seguridad financiera o la reputación, en general, no se consideran amenazas inminentes y graves (107).

Principio 7: revelación de información a los procesadores de datos

El controlador de datos puede usar procesadores de datos para el procesamiento de datos personales. Ello no se considerará divulgación de infor-

mación a terceros, que exigiría la notificación a la persona cuyos datos se procesan, si media una de las condiciones siguientes.

El controlador de datos asegura el nivel de protección

No constituirá una divulgación a terceros si el controlador de datos se asegura de que el procesador de datos ofrece, como mínimo, el mismo nivel de protección que exige la legislación nacional y las protecciones que constan en el presente documento (108).

Nivel de protección establecido por una relación contractual

No constituirá una divulgación a terceros si el controlador de datos y el procesador de datos establecen una relación contractual que determine el deber del procesador de datos de cumplir con las instrucciones del controlador de datos, en las que se determine el deber de aquél de cumplir con las instrucciones de este, que deben garantizar la adecuada protección de los datos personales (109). El contrato también debe establecer las medidas de seguridad adecuadas para garantizar la protección de los datos personales (110). Asimismo, una vez caducada la relación contractual, el procesador de datos debe destruir debidamente los datos personales o devolverlos al controlador de datos (111).

Debería existir como mínimo la autorización previa del titular para realizar este tipo de transferencias a terceros.

Principio 8: transferencias internacionales

Las transferencias internacionales de datos personales sólo deberán efectuarse cuando el exportador de los datos se hace responsable de la protección de la información o si el país receptor (país de destino) ofrece, como mínimo, el mismo nivel de protección de los datos personales que brindan estos principios, o cuando existan otras razones legítimas para el procesamiento de los datos (112). Además, los países de tránsito, que son países por los que la información pasa pero no es procesada, no tienen obligación de cumplir dichos requisitos (113). Pero, no obstante, la transferencia de datos personales debe ser segura.

Para determinar si el país receptor otorga las normas mínimas de protección de datos, deben analizarse los factores siguientes: 1) la naturaleza de los datos; 2) el país de origen; 3) el país receptor; 4) el propósito para el cual se procesan los datos, y 5) las medidas de seguridad vigentes para la transferencia y el procesamiento de los datos personales (114) En caso de que el país receptor no otorgue el mismo nivel de protección, podría aun así efectuarse la transferencia, si media alguna de las condiciones siguientes y si el procesamiento es justo y legítimo (115). Es importante señalar tam-

bién, sin embargo, que algunos países han expresado reservas en cuanto a la regulación de las transferencias internacionales aludiendo al concepto de protección equivalente en el país receptor.

Este enfoque ha resultado ser difícil de aplicar en la práctica y en la actualidad es objeto de debate en el contexto de la revisión de la Directiva Europea. Cualesquier principios y recomendaciones deben reconocer que la información personal debe ser protegida en el contexto de las transferencias internacionales, pero debe seguir siendo flexible en cuanto a la forma de lograrlo.

Rendición de cuentas

En concordancia con los principios relativos a la rendición de cuentas, cuando las leyes locales no revean la protección adecuada de los datos importados, la transferencia se llevará a cabo sólo si el exportador se hace responsable de la protección de los datos personales independientemente de su ubicación geográfica y si está dispuesto y está en posibilidad de dar pruebas fehacientes de ello cuando se le requiera (116).

Una relación contractual garantiza el nivel de protección

Los datos personales podrían transferirse a un país receptor que no otorga, como mínimo, el mismo nivel de protección de los datos personales que ofrecen estos principios, si existe una cláusula contractual que obliga al cumplimiento del nivel mínimo de protección de los datos (117).

La legislación nacional permite la transferencia internacional

La legislación nacional podría permitir la transferencia de datos personales a un tercer país que no otorgue el mismo nivel de protección si media alguna de las condiciones siguientes: 1) la transferencia es necesaria y en beneficio de la persona en una relación contractual; 2) la transferencia es necesaria para proteger un interés vital, como evitar un daño sustancial o la muerte de la persona o de un tercero; 3) la transferencia está autorizada legalmente para proteger un interés público, o 4) el exportador de los datos se responsabiliza de la protección de los mismos (118).

Consentimiento

Puede admitirse la transferencia de datos personales a un país receptor que no otorga el mínimo nivel de protección si la persona afectada consiente inequívocamente la transferencia (119).

Innovación tecnológica

Las normas que rigen la transferencia de datos e información entre países deben reflejar la realidad manifiesta en el uso de la Internet, además de que deben tomar en cuenta el hecho de que las restricciones a la transferencia de datos puede limitar la innovación tecnológica y el desarrollo económico.

Principio 9: derecho de la persona al acceso a la información

El derecho de acceso es el derecho de la persona a solicitar y obtener del controlador de datos información sobre sus datos personales (120). La persona podría no tener derecho de acceso a los datos personales si media la probabilidad de que la divulgación tenga un efecto no razonable para la privacidad y los derechos de un tercero, a menos que se suprima la información sobre el tercero o éste consienta en la divulgación (121). Corresponde señalar que el derecho de acceso otorga a la persona la posibilidad de ver la información sobre sus datos personales y no los documentos que la contengan (122).

Datos personales que pueden ser solicitados y divulgados

Una persona puede solicitar información sobre un dato personal específico o sobre cómo y por qué se procesa el dato personal (123). Esto último incluye información sobre la fuente de los datos personales, el propósito del procesamiento y para quién se efectúa, lo cual puede incluir la categoría de receptores a los que se divulgarán los datos personales (124). A menos que los datos personales sean enmendados o suprimidos como rutina, el controlador de datos debe revelar los datos personales en su poder a la fecha de la solicitud (125). Sin embargo, si los datos personales son enmendados o suprimidos regularmente, el controlador de datos puede, en su defecto, revelar los datos personales que estén en su poder en el momento de responder a la solicitud (126).

Cómo y cuándo deben divulgarse los datos personales

Conforme lo requiere el principio de transparencia señalado, toda la información que se suministre a la persona afectada debe ser clara y fácilmente comprensible (127) El controlador de datos puede suministrar copia de los datos personales o exhibir los datos personales para que los inspeccione la persona afectada. Además, el controlador de datos puede suministrar información sobre datos personales a una persona gratuitamente o previo pago de un cargo que no sea excesivo (128).

Asimismo, la legislación nacional puede exigir que el controlador de datos responda a las solicitudes de datos personales dentro de un plazo razonable, conforme a la cantidad y el tipo de información sobre datos personales solicitada (129).

Solicitudes repetidas

La legislación nacional podría limitar el número de veces durante un período que el controlador de datos debe responder a solicitudes de datos personales de una misma persona (130). El objetivo de esta norma es limitar las solicitudes repetidas formuladas por una persona durante un breve

período.131 Sin embargo, si una persona presenta una razón legítima para solicitar reiteradamente acceso a sus datos personales, el controlador de datos podría, aún así, tener que responder (132).

Limitaciones

El derecho de acceso debería estar sujeto a ciertas limitaciones razonables. Por ejemplo, los controladores deberían tener la posibilidad de negar el acceso si la persona que lo solicita es incapaz de verificar su identidad como la persona con quien se relaciona la información que solicita; si como consecuencia de ello se revelaría información, tecnología o procesos operativos confidenciales o exclusivos, o si fuese ilícito revelar la información o pudiese interferir con la detección y prevención de una actividad ilegal.

Principio 10: derecho de la persona a corregir y suprimir sus datos personales

La persona tiene derecho a solicitar que el controlador de datos corrija o suprima los datos personales que puedan ser "incompletos, inexactos, innecesarios o excesivos".133 Mientras el controlador de datos está en proceso de corrección o supresión, éste puede bloquear el acceso o indicar que los datos personales están bajo revisión, antes de divulgar su contenido a terceros (134).

Correcciones y supresiones razonables

Si la corrección o supresión es razonable, el controlador de datos debe corregir o suprimir los datos personales a solicitud de la persona afectada.135 Si los datos personales han sido divulgados a terceros, el controlador de datos debe también notificar a estos del cambio, si los conoce (136).

Correcciones y supresiones no razonables

Si la persona solicita la corrección o supresión de datos personales y éstos deben ser retenidos para el cumplimiento de un deber impuesto al controlador de datos por la legislación nacional o debido a una relación contractual entre el controlador de datos y la persona afectada, no se considerará razonable la corrección o supresión.137 En algunos casos, particularmente cuando los datos pueden encontrarse en varios servidores en línea, algunos de los cuales estén fuera del alcance del controlador de datos, tal vez no sería técnicamente posible borrar todos los datos, por lo que su eliminación debería ampliarse sólo a lo comercialmente factible. Además, en el caso de servicios en línea, los derechos del usuario se aplican sólo a sus propios datos (es decir, aquellos que el mismo usuario haya capturado y que conserve el proveedor de servicios. Sin embargo, este derecho no se aplica a aquellos datos generados durante la operación del servicio.

Principio 11: derecho a objetar el procesamiento de datos personales

La persona podría objetar el procesamiento de sus datos personales en los casos en que exista una razón legítima, como un perjuicio o angustia injustificada y sustancial para ella (138). La persona debe especificar por qué el procesamiento de sus datos personales tiene ese efecto (139). Sólo puede objetar el procesamiento de sus propios datos personales (140) y no podrá objetarlos si son necesarios para el cumplimiento de un deber impuesto al controlador de datos por la legislación nacional o para la ejecución de una obligación contractual entre la persona y el controlador de datos, o si la persona expresó su consentimiento (141).

Principio 12: legitimación para ejercer los derechos sobre el procesamiento de datos personales

Las personas y los terceros representantes pueden ejercer el derecho de acceso, el derecho de corrección y supresión y el derecho a objetar el procesamiento de datos personales (142).

La persona

La persona puede ejercer el control directo sobre sus propios datos personales (143). El controlador de datos puede requerir que la persona suministre información razonable para determinar su identidad (144).

Terceros representantes

La legislación nacional puede permitir la legitimación de herederos para ejercer los derechos sobre los datos personales de un individuo, en caso de fallecimiento de este (145). Además, los abogados y otras personas que actúen en nombre de la persona afectada pueden estar legitimados para ejercer los derechos sobre los datos personales de un individuo (146). Sin embargo, el controlador de datos debe quedar debidamente satisfecho de que los terceros tienen la autoridad correspondiente para actuar en nombre de la persona afectada (147).

Procedimiento para el ejercicio de los derechos

El controlador de datos debe contar con procedimientos establecidos que permitan que las personas ejerzan el derecho de acceso, el derecho de corrección y supresión y el derecho de objeción, de manera fácil, rápida y eficiente.148 Además, los procedimientos no deben comportar demoras o costos innecesarios, ni aportar ventaja alguna para el controlador de datos (149).

Legislación nacional que limite y niegue el ejercicio de los derechos

La legislación nacional puede limitar o negar la capacidad de una persona o de sus representantes a ejercer el derecho de acceso, el derecho de corrección y supresión y el derecho de objeción. (150). Sin embargo, el controlador de datos debe informar a la persona o a sus representantes las razones en que se funda la decisión de limitar o negar el ejercicio de esos derechos, a menos que ello vaya en detrimento de la investigación de una actividad ilícita (151).

Principio 13: medidas de seguridad para proteger los datos personales

El controlador de datos y el procesador de datos deben disponer de "medidas técnicas y organizacionales" razonables para garantizar la integridad, confidencialidad y disponibilidad de los datos personales (152). Estas medidas dependerán de cómo se procesen los datos personales, de las consecuencias de una violación para las personas afectadas, de la sensibilidad de la información y de todo deber impuesto por la legislación nacional (153). Además, el controlador de datos debe tomar medidas razonables para destruir, disponer o retirar en forma permanente de los datos personales toda información sobre identificación que ya no sea necesaria para su procesamiento (154).

Violaciones de la seguridad

El controlador de datos debe informar a la persona afectada de toda violación de la seguridad que pueda afectar sustancialmente sus derechos y toda medida que se adopte para subsanar la violación (155). La información debe ser suministrada en un tiempo razonable para que la persona afectada pueda tomar medidas para proteger sus derechos.156 Por el contrario, el requerimiento de aviso en caso de que una violación no represente una amenaza seria daría lugar a la emisión de avisos de poca importancia, que los individuos afectados considerarían poco serios (aunque ello implique un riesgo de daño serio).

Principio 14: deber de confidencialidad

Los controladores de datos y los procesadores de datos tienen el deber de mantener la confidencialidad de todos los datos personales.157 El deber de confidencialidad se extiende hasta después de terminada la relación entre la persona y el controlador de datos, o entre el procesador de datos y el controlador de datos.158 Sin embargo, el deber de confidencialidad puede

quedar en manos de la justicia, de ser necesario para proteger la seguridad pública, la seguridad nacional o la salud pública (159).

Principio 15: control, cumplimiento y responsabilidad

Para asegurar el cumplimiento y la aplicación de los principios de la protección de datos, los Estados Miembros de la OEA deben contar con una autoridad supervisora y establecer un recurso judicial para las personas. Además, los controladores de datos y los procesadores de datos que no procesen los datos personales conforme a lo previsto en la legislación nacional aplicable podrían ser sujetos a responsabilidad administrativa, civil o penal.

Los Estados Miembros de la OEA deben unir esfuerzos para garantizar con certeza y predicibilidad que habrá una autoridad supervisora con jurisdicción sobre determinadas actividades de procesamiento de datos. La jurisdicción o aplicación simultánea de normas nacionales opuestas puede representar una carga irracional para los controladores y ello dificultará la transparencia y la protección de los derechos del individuo.

Autoridad de supervisión

Los Estados Miembros de la OEA deben contar con una autoridad que sea responsable de la supervisión del cumplimiento de estos principios de la protección de datos y de la legislación nacional aplicable con respecto a las actividades de procesamiento sobre las que tienen jurisdicción (160). La autoridad encargada de la supervisión debe ser imparcial e independiente (161).

Asimismo, debe contar con capacidad técnica, facultades y recursos suficientes para realizar investigaciones y auditorías a fin de asegurar el cumplimiento de las normas pertinentes (162). Asimismo, debe estar en condiciones de imponer sanciones financieras por incumplimiento (163) La autoridad encargada de la supervisión debe estar facultada para manejar denuncias en que se alegue la violación de la protección de los datos y prever reparaciones administrativas para las personas afectadas (164).

Asimismo, se podría exigir a una organización que proyecte procesar datos personales sumamente sensibles o participar en procesamiento de alto riesgo que comunique su intención de hacerlo a la autoridad supervisora, antes de permitirse el comienzo del procesamiento (165) También se podría exigir que los controladores de datos comuniquen a la autoridad supervisora todo cambio en el uso y los propósitos de su procesamiento de datos personales (166).

La legislación nacional podría asignar a la autoridad supervisora la facultad de permitir o negar algunas o todas las transferencias internacionales

de datos personales dentro de su jurisdicción (167). Sin embargo, la autoridad puede permitir al procesador de datos que transfiera la información pertinente mientras éste se responsabilice del procesamiento y protección adecuados de los datos después de haber sido transferidos a un país que no cumpla con los requerimientos dispuestos en las normas nacionales. Los controladores de datos personales que se propongan transferir datos personales a terceros países deben estar en condiciones de demostrar ante la autoridad supervisora que la transferencia cumple con estos principios y con la legislación nacional aplicable (168).

Recurso judicial

Sin perjuicio de todo recurso administrativo que otorgue la autoridad supervisora, las personas deben también tener un recurso ante el sistema judicial nacional para hacer valer los derechos de protección de los datos personales que les otorga la legislación nacional (169) De acuerdo con la legislación aplicable, la persona afectada puede tener derecho a una indemnización por daños si sufre un perjuicio porque el controlador de datos no protegió sus datos personales (170). Además, la justicia también podría brindar una instancia de revisión judicial de las decisiones administrativas de la autoridad supervisora, (171) y algunas violaciones graves de las protecciones de los datos personales previstas en la legislación nacional podrían ser encausadas como delitos penales (172)

Conflictos entre leyes

Los Estados Miembros de la OEA deben unir esfuerzos para garantizar con certeza y previsibilidad que habrá una autoridad supervisora con jurisdicción sobre determinadas actividades de procesamiento de datos. La jurisdicción o aplicación simultánea de normas nacionales opuestas puede representar una carga irracional para los controladores y ello dificultará la transparencia y la protección de los derechos del individuo. Por el contrario, la existencia de reglas claras y coherentes para determinar la jurisdicción de una autoridad ayudará a evitar confusiones y cargas innecesarias a los controladores que de otro modo se verían ante la obligación de notificar a varias autoridades, conforme a diversos sistemas jurídicos, por una sola actividad de procesamiento (173).

VI. MEDIDAS PROACTIVAS Y COOPERACIÓN

Los Estados Miembros de la OEA, conscientes de la discrepancia entre la regulación y la tecnología, deberían considerar la adopción de medidas proactivas y de cooperación para promover la protección de los datos personales. Estas se harán cada vez más necesarias a medida que evolucione la

tecnología y los Estados Miembros de la OEA queden más interconectados tecnológicamente, entre sí y con otros países de otras regiones del mundo.

Medidas proactivas

En consecuencia, los Estados Miembros de la OEA deberían considerar la creación y ejecución de programas de capacitación, educación y fomento de la conciencia pública para la ciudadanía en general y para funcionarios del Estado, con objeto de fomentar la comprensión de la legislación, los procedimientos y los derechos en materia de protección de los datos personales (174).

Los Estados Miembros de la OEA también deberían crear procedimientos operativos normalizados para los controladores de datos, a fin de prevenir, detectar y contener las posibles violaciones de la seguridad (175). Los Estados Miembros deben estimular las auditorías a cargo de una entidad independiente o de la sociedad civil para evaluar y verificar que cumplan con las leyes aquellos controladores que se hayan arriesgado por haber violado deliberadamente o por accidente las leyes de protección de datos en el pasado (176). Además, los Estados Miembros deberían fomentar la creación de grupos de trabajo y la celebración de seminarios y talleres destinados a promover e intercambiar prácticas óptimas sobre protección de los datos personales (177).

Cooperación

También debería estimularse a las autoridades nacionales encargadas de la protección de los datos personales a cooperar y coordinar entre sí en el ámbito nacional e internacional para promover la protección uniforme y adecuada de los datos personales (178). Los controladores y procesadores de datos que operen en varios mercados deberían estar sujetos a una sola ley y una sola autoridad supervisora. En tales casos, esta autoridad supervisora debe cooperar con las autoridades de otras jurisdicciones a fin de garantizar una efectiva implementación de estas normas. En el caso de una investigación, debe alentarse a las autoridades nacionales a cooperar y coordinar entre sí y con los organismos internacionales (179). Como ocurre con los principios antes enumerados, la cooperación entre las autoridades nacionales y las autoridades internacionales es parte esencial de la protección de los datos personales.

Conclusiones del Comité Jurídico Interamericano

El CJI, en su informe de 2007 sobre el tema, brindó las conclusiones siguientes: "La protección de la información y los datos de carácter personal que se mantienen en forma electrónica en el sector privado ha avanzado merced a la creación de instrumentos internacionales. Las Directrices de las OCDE, el Convenio del Consejo de Europa, las Directrices de las Na-

ciones Unidas y, particularmente, la Directiva de la UE para la protección de los datos, han tenido un profundo impacto en la protección de datos en Europa y en otras regiones. Asimismo, algunos países miembros de la OEA, en particular Canadá y Chile, han aprobado leyes que brindan niveles relativamente elevados de protección de la privacidad. Sin embargo, parece justo decir que muchas de las dificultades subsisten, en particular con respecto al flujo transfronterizo de datos personales por Internet y otras redes mundiales. La privacidad de los ciudadanos sigue siendo vulnerable aún en los países que cuentan con legislaciones nacionales efectivas debido a la existencia de "paraísos" de datos donde no se dispone de protección. Los instrumentos internacionales y nacionales vigentes dejan numerosos problemas sin resolver, como la interpretación de qué niveles de protección son "adecuados" y "equivalentes" o la naturaleza de los mecanismos necesarios para hacer cumplir las normas acordadas. La legislación y las formas de hacerla cumplir son especialmente complejas debido a la vertiginosa evolución de la tecnología. Además, los Estados que desean proteger la privacidad de sus ciudadanos también enfrentan la competencia de intereses económicos, comerciales, sociales y políticos.

Sin embargo, esas dificultades no existen sólo en la esfera de la protección de los datos. Tal vez se avanzaría más en la esfera de la protección de la privacidad mediante una combinación de medidas, como la elaboración de normas internacionales y de mecanismos para hacerlas cumplir, la asistencia jurídica y técnica mutua, el estímulo de la autorregulación de la industria y la operación de las fuerzas del mercado bajo la influencia de la información y la educación."

Conclusión

Finalmente, los Estados Miembros de la OEA debieran seguir estudiando el tema y considerar la posibilidad de actualizar sus sistemas regulatorios de protección de los datos personales con base en los principios y recomendaciones que se describen en el presente trabajo, centrándose primordialmente en salvaguardar el derecho a la privacidad de las personas sin privar al individuo ni a la sociedad de los beneficios derivados de la continua innovación y de los servicios prestados a través de Internet. Esas normas deberían regir en todas las circunstancias de recolección, custodia, control y transferencia de datos por parte de entidades públicas o privadas. También deberían regir en todas las circunstancias en que un tercero pueda tener derecho a acceder a esa información al amparo de la legislación pertinente.

Los legisladores en todo el mundo están evaluando si sus marcos jurídicos están al día con respecto a los avances tecnológicos de tal manera que queden protegidos los datos privados de las personas y, al mismo tiempo,

promuevan el desarrollo económico y la innovación tecnológica. Estos principios y estas recomendaciones preliminares han servido de base para la legislación sobre protección de datos en distintas partes del mundo y puede servir de fundamento para un nuevo instrumento internacional o una legislación nacional sobre la protección de datos en las Américas.

Comentarios de MÉXICO

MISIÓN PERMANENTE DE MÉXICO

OEA-00839

La Misión Permanente de México ante la Organización de los Estados Americanos (OEA) saluda atentamente a la Secretaria General de la OEA Departamento de Derecho Internacional – y hace referencia al "Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales".

AI respecto, el gobierno de México considera aceptable en lo general el proyecto de estudio preliminar, toda vez que es un documento que consideramos contiene todos los principios que los Estados deben tomar en cuenta para normar su legislación, y que puede servir como fundamento para un nuevo instrumento Internacional sobre la protección de los datos en las Américas.

Tal y como lo reconoce el documento, México cuenta ya con un instrumento normativo nacional a partir de 2010 (Ley Federal de Protección de Datos Personales en Posesión de los Particulares DOF 5-julio-2010) el cual recoge en su gran mayoría los principios que contiene el estudio preliminar presentado por el Departamento de Derecho Internacional de la OEA. De igual manera, México cuenta con lineamientos de protección de datos personales publicados en el Diario Oficial el 30 de septiembre de 2005, los cuales tienen por objeto establecer las políticas generales y procedimentales que deberán reservar las dependencias y entidades de la Administración Publica Federal para garantizar a la persona la facultad de decisión sobre el use y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.

A la Secretaría General
Departamento de Derecho Internacional

Organización de los Estados Americanos
Washington, D.C.

Una tarea para la OEA Sera definir la naturaleza de un futuro instrumento interamericano que sea de utilidad para sus Estados Miembros en el desarrollo del derecho a la protección de datos personales. De manera preliminar, se estima que dicho proyecto debe contener un capitulo de definiciones claras y precisas, toda vez que puede afectar la interpretación de la Legislación en materia de protección de datos. En ese sentido, se considera oportuno incluir una definición del "controlador de datos". En el precepto se alude a definiciones contenidas en diversas legislaciones, sin concluir o apuntar la extensión y alcance del concepto. Al efecto, entre otros, se menciona la definición del Convenio y las Directrices sabre protección de la privacidad y flujos fronterizos de datos personales de la Organización para la Cooperación y el Desarrollo Económico, que abarca tanto a personas físicas coma a personas morales.

En el proyecto se indica que en aras de transparencia debe divulgarse los datos del controlador de datos. El Gobierno de México considera que los datos a revelar son los correspondientes a la unidad que funja como responsable del control de datos y no necesariamente los de la persona física o moral que en lo específico realiza dicha función.

En relación con el principio 8 relativo a la transferencia internacional de datos personales, se considera apropiado que los Estados puedan no transferir datos a otros que no cuenten con una legislación con el mismo nivel de protección de los datos. Sin embargo, seria factible contemplar que el Estado que remite la información también pudiera condicionar el uso, destino y posible ulterior transferencia de dicha información, incluso requiriendo la obtención de su aquiescencia con antelación. Adicionalmente, la propuesta actual parecería imponer la obligación a todos los Estados de conocer derecho extranjero y sus alcances particulares, lo que podría dificultar el intercambio.

Por otra parte, en anexo se remiten los comentarios del Instituto Federal de Acceso a la información y Protección de Datos (IFAI) de México.

La Misión Permanente de México ante la OEA aprovecha la oportunidad para renovar a la Secretaria General de la OEA--Departamento de Derecho Internacional-las seguridades de su consideración distinguida.

Washington, D.C., 15 de abril de 2011

Comentarios de ESTADOS UNIDOS

REPRESENTANTE PERMANENTE DE ESTADOS UNIDOS

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

DEPARTMENTODE ESTADO

Washington, D. C. 20620

5 de mayo de 2011

Señor Jean Michel Arrighi
Secretario de Asuntos Jurídicos
Organización de los Estados Americanos Washington, D. C. 20006

Señor Arrighi:

La Misión Permanente de Estados Unidos ante la Organización de los Estados Americanos saluda atentamente a la Secretaría de Asuntos Jurídicos y se complace en hacer referencia a la solicitud de comentarios sobre el Proyecto de Principios y Recomendaciones sobre la Protección de Datos ("el Proyecto") hecha en la sesión especial de la Comisión de Asuntos Jurídicos y Políticos sobre el tema "acceso a la información pública", el 13 de diciembre de 2010, en Washington, D. C.

Estados Unidos se permite expresar su agradecimiento al Departamento de Derecho Internacional de la OEA por haber elaborado este Proyecto.

El Gobierno de Estados Unidos está muy comprometido con la protección de la información personal y participa activamente en los debates que sobre este y otros temas conexos se llevan a cabo en varios foros internacionales. Nos hemos permitido compartir este Proyecto con expertos en la materia de los Departamentos de Estado, Comercio, Justicia, Seguridad Nacional, así como con la Comisión Federal de Comercio de nuestro país. Estados Unidos agradece las contribuciones de este Proyecto inicial. Sin embargo, considera que debe hacerse un estudio adicional en el que se tome en cuenta la amplia gama de enfoques y esfuerzos internacionales en materia de protección de datos (por ejemplo, los llevados a cabo por APEC y OCDE). Considera asimismo que deberían estudiarse con mayor detalle las leyes y reglamentos sobre el tema, existentes en los Estados Miembros de la OEA, incluso los de Estados Unidos.

El tema de la privacidad de los datos es sumamente complejo y técnico, sobre el que quedan por debatir importantes aspectos de índole política y reglamentaria. La Comisión de Derecho Internacional de las Naciones Unidas ha señalado que la protección de datos es "un área incipiente en los Estados". Como tal, consideramos que es prematuro tratar de transformar esta área relativamente subdesarrollada en principios o recomendaciones para los países del continente. Consideramos además que nuestros recursos deberían ser dedicados mejor a un examen más amplio de las leyes nacionales e instrumentos internacionales existentes y al análisis de los esfuerzos regionales e internacionales en la materia. Un esfuerzo de esta naturaleza proporcionaría una base más firme para evaluar la conveniencia y posible contenido de unos principios y recomendaciones de la OEA sobre esta materia.

La Misión Permanente de Estados Unidos aprovecha esta oportunidad para reiterar a la Secretaría de Asuntos Jurídicos las seguridades de su más alta y distinguida consideración.

Atentamente,
Carmen Lomellin
Embajadora
Cc: Dante Negro
Director, Departamento de Derecho Internacional

NOTAS AL PIE

1 Jean Sleemons Stratford y Juri Stratford, Data Protection and Privacy in the United States and Europe, IASSIST QUARTERLY, otoño de 1998, pág. 19.
2 Id. pág. 17.
3 Id.
4 Id. pág. 19.
5 Véase Consejo de Europa, Convenio para la Protección de Individuos con respecto al Proceso Automatizado de Datos Personales, arts. 2, 4-12, 28 de enero de 1981.
6 Véase Stratford, supra, pág. 19 (donde se agrega que la Directiva, que fue aprobada en 1995, encomendaba a los Estados miembros asegurar que su legislación nacional sobre privacidad cumpliera con sus normas).
7 Id.
8 Id. págs. 19 y 20.

9 Id. pág. 17.
10 Id. (en donde se cita a Samuel Warren y Louis Brandeis, quienes argumentaban que el derecho a la privacidad otorgado a la "propiedad intelectual y artística" en el derecho consuetudinario de Estados Unidos se "fundaba en el de la 'personalidad inviolable'").
11 Id.
12 Id.
13 Id.
14 Id. págs. 17 a 19 (en donde se señala que la Ley de Privacidad y la Ley de comparación electrónica de datos y protección de la privacidad, de 1988, son los dos instrumentos legislativos más importantes de los Estados Unidos para la protección del derecho a la privacidad y de los datos personales).
15 Véase también id. pág. 19.
16 Véase Preliminary FTC Staff Privacy Report: Remarks of Chairman Jon Leibowitz, 1 de diciembre de 2010, http://www.ftc.gov/speeches/leibowitz/101201privacyreportremarks.pdf.
17 Id. págs. 19 y 20.
18 Véase Stratford, supra, pág. 20.
19 Andreas Guadamuz, Habeas Data: An update on the Latin American data protection constitutional right, BILETA, 4 de enero de 2005, http://www.bileta.ac.uk/01papers/guadamuz.html.
20 Véase id.; Pablo Palazzi, El Habeas Data en el Derecho Argentino, Revista de Derecho Informático, noviembre de 1998, http://www.alfa-redi.org/rdi-articulo.shtml.
21 Véase Gaudamuz, supra.
22 Id. (donde se señala que los datos personales sensibles incluyen la religión, las ideologías políticas y la orientación sexual); Palazzi, supra (donde se afirma que el habeas data argentino requiere pruebas de información inexacta o discriminación para corregir, rectificar o suprimir datos personales).
23 Id.
24 Id. (donde se indica que el habeas data de Argentina no permite que una persona agraviada acceda a los datos personales de un tercero, aunque pueda existir un vínculo entre los datos personales de ambos).
25 Id.
26 Véase también Ley de protección de datos personales de Argentina No. 25.326, § 14, supra.
27 Consejo de Europa, supra, art. 2; véase Organización para la Cooperación y el Desarrollo Económicos (OCDE), Directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales, art. 1, 23 de septiembre de 1980 (donde se señala que en los comentarios detallados del grupo de

expertos se afirma que las Directrices versaban sobre los datos personales de "personas físicas").

28 Agencia Española de Protección de Datos, Estándares Internacionales sobre Protección de Datos Personales y Privacidad: Resolución de Madrid, 5 de noviembre de 2009.

29 Ley de protección de datos personales de Argentina No. 25.326, § 1 (30 de octubre de 2000).

30 Véase Oficina del Comisionado de Información, Guía de la protección de datos, pág. 22 (en donde se agrega que las opiniones u otras expresiones de intención sobre la persona son también datos personales). Agencia CP27331S04 Española de Protección de Datos, supra (en donde se definen los "datos personales" como "toda información relacionada con una persona natural identificada").

31 Organización para la Cooperación y el Desarrollo Económicos, supra, art. 1

32 Consejo de Europa, supra, art. 2

33 Véase Oficina del Comisionado Federal para la Privacidad, Directrices para los principios nacionales sobre privacidad, 23 (septiembre de 2001) (en donde se observa que esta legislación se aplica a organizaciones privadas); Ley de protección de la información personal y de los documentos electrónicos, 13 de abril de 2000, art. 2 (Can.) (en donde se observa que esta legislación se aplica a organizaciones privadas); Oficina del Comisionado de Información, supra, pág. 23; Ley orgánica 15/1999 del 13 de diciembre sobre la protección de datos personales, art. 7 (13 de diciembre de 1999) (España). Véase también Ley de privacidad, 1 de junio de 2009, art. 3 (Can.); Comisionado para la Privacidad, Plain English Guidelines to Information Privacy 1 (1994) (en donde se observa que la Ley canadiense sobre privacidad y los Principios de privacidad de la información, de Australia, se aplican al Estado).

34 Véase Oficina del Comisionado de Información, supra, pág. 27; Ley orgánica, supra, art. 3.

35 Id.

36 Véase Oficina del Comisionado de Información, supra, pág. 28.

37 Id. pág. 29.

38 Id. pág. 23; Ley orgánica, supra, art. 7.

39 Véase Consejo de Europa, supra, art. 2.

40 Véase Oficina del Comisionado de Información, supra, pág. 25.

41 Véase Agencia Española de Protección de Datos, supra.

42 Id.

43 Véase Oficina del Comisionado de Información, supra, pág. 25.

44 Id.

45 Véase Agencia Española de Protección de Datos, supra.

46 Véase Ley orgánica, supra, art. 2.
47 Véase Oficina del Comisionado de Información, supra, pág. 115.
48 Id.
49 Id.
50 Véase Agencia Española de Protección de Datos, supra.
51 Véase Oficina del Comisionado de Información, supra, pág. 115.
52 Véase Comisionado para la Privacidad, Plain English Guidelines to Information Privacy: Principios 8 a 11, supra, pág. 29.
53 Véase Oficina del Comisionado de Información, supra, pág. 116.
54 Id.
55 Id. pág. 51; Comisionado para la privacidad, supra, pág. 11.
56 Véase Oficina del Comisionado de Información, supra, pág. 51.
57 Véase Agencia Española de Protección de Datos, supra.
58 Véase Oficina del Comisionado de Información, supra, pág. 43.
59 Id. págs. 43, 45 (en donde se señala que, en ciertas ocasiones, el procesamiento de datos personales puede
tener efectos adversos en una persona pero no se considerará injusto si, por ejemplo, se relaciona con un propósito legítimo, como hacer cumplir la ley).
60 Véase Oficina del Comisionado de Información, supra, págs. 43, 46.
61 Id. págs. 43, 47 (donde se agrega que, para que los datos personales puedan ser procesados en forma justa, las notificaciones relacionadas con la privacidad deben incluir la identidad de quien está recabando los datos personales, el uso proyectado de los mismos y toda otra información que deba ser revelada al individuo).
62 Id. pág. 47.
63 Véase Agencia Española de Protección de Datos, supra.
64 Véase Oficina del Comisionado de Información, supra, pág. 54.
65 Id. pág. 53. Véase también Oficina del Comisionado Federal para la Privacidad, supra, pág. 36 (en donde se afirma que la prueba de una "expectativa razonable" debe ser "lo que esperaría una persona sin conocimientos especiales de la industria o actividad implícita").
66 Véase Oficina del Comisionado Federal para la Privacidad, supra, pág. 33
67 Véase Agencia Española de Protección de Datos, supra.
68 Véase Oficina del Comisionado de Información, supra, págs. 54, 56.
69 Véase Oficina del Comisionado Federal para la Privacidad, supra, pág. 35
70 Id.
71 Véase Agencia Española de Protección de Datos, supra.
72 Véase Comisionado para la Privacidad, Plain English Guidelines to Information Privacy: Principios 1 a 3, supra, pág. 6.

73 Véase Oficina del Comisionado de Información, supra, pág. 59 (en donde se observa que, si determinada información personal es necesaria sólo en relación con ciertas personas, la recolección y el procesamiento de esa información en relación con otras se considerará excesivo).
74 Id.
75 Véase Organización para la Cooperación y el Desarrollo Económicos, supra, art. 10.
76 Véase Agencia Española de Protección de Datos, supra.
77 Véase Oficina del Comisionado Federal para la Privacidad, supra, pág. 27 (en donde se agrega que no es aceptable la recolección de datos personales por la remota posibilidad de que sean necesarios en el futuro).
78 Véase Comisionado para la Privacidad, Plain English Guidelines to Information Privacy: Principios 1 a 3, supra, pág. 6.
79 Véase Oficina del Comisionado de Información, supra, pág. 114.
80 Véase Ley de protección de datos del Reino Unido, 1998, § 1.
81 Véase Oficina del Comisionado de Información, supra, pág. 61.
82 Id. pág. 7.
83 Véase Agencia Española de Protección de Datos, supra.
84 Véase Comisionado para la Privacidad, Plain English Guidelines to Information Privacy: Principios 1 a 3, supra, pág. 17.
85 Véase también Oficina del Comisionado de Información, supra, pág. 8.
86 Véase Agencia Española de Protección de Datos, supra.
87 Id.
88 Id.
89 Id.
90 Véase Ley de protección de datos personales de Argentina No. 25.326, supra, § 15.
91 Véase Oficina del Comisionado de Información, supra, pág. 125.
92 Véase Agencia Española de Protección de Datos, supra; Oficina del Comisionado de Información, supra, pág.
93 Véase Agencia Española de Protección de Datos, supra.
94 Id.
95 Véase Comisionado Federal para la Privacidad, supra, págs. 47 y 48.
96 Véase Agencia Española de Protección de Datos, supra; Oficina del Comisionado de Información, supra, pág.112.
97 Véase Agencia Española de Protección de Datos, supra.
98 Id.
99 Véase Oficina del Comisionado de Información, supra, pág. 111.
100 Véase Agencia Española de Protección de Datos, supra.

101 Id.
102 Id.
103 Véase Oficina del Comisionado Federal para la Privacidad, supra, pág. 41
104 Véase Agencia Española de Protección de Datos, supra; Comisionado para la Privacidad, Plain English Guidelines to Information Privacy: Principios 8 a 11, supra, pág. 38.
105 Véase Comisionado para la Privacidad, Plain English Guidelines to Information Privacy: Principios 8 a 11, supra, pág. 37.
106 Id. pág. 22.
107 Véase Oficina del Comisionado Federal para la Privacidad, supra, pág. 40
108 Véase Agencia Española de Protección de Datos, supra.
109 Id.; Véase Ley orgánica, supra, art. 12 (donde se observa que el procesador de datos es responsable de toda divulgación de datos personales que no esté de acuerdo con el contrato).
110 Véase Ley orgánica, supra, art. 12.
111 Id.
112 Véase Agencia Española de Protección de Datos, supra.
113 Véase Oficina del Comisionado de Información, supra, pág. 95.
114 Véase Ley de protección de datos del Reino Unido, 1998, § 8, supra.
115 Véase Oficina del Comisionado de Información, supra, pág. 94.
116 En Marco APEC que ahora están creando los países de la Cuenca del Pacífico se hace uso explícito de un modelo basado en la rendición de cuentas, junto con el consentimiento, para la transferencia de datos. Tal como se indicó anteriormente, Europa también está revisando sus reglamentos en materia de transferencia de datos (que datan de hace más de 15 años); y muchas partes interesadas han solicitado también un cambio hacia un régimen de transferencia basado en la rendición de cuentas_. http://publications.apec.org/publication-detail.php?pub_id=390.
117 Véase Agencia Española de Protección de Datos, supra.
118 Véase también id.
119 Véase Oficina del Comisionado para la Privacidad, supra, pág. 58.
120 Véase también Agencia Española de Protección de Datos, supra.
121 Véase Ley de protección de la información y los documentos electrónicos, supra, art. 8; Oficina del Comisionado Federal para la Privacidad, supra, pág. 50; Oficina del Comisionado de Información, supra, pág.133.
122 Véase Oficina del Comisionado de Información, supra, pág. 123.
123 Véase Agencia Española de Protección de Datos, supra.
124 Id.
125 Véase Oficina del Comisionado de Información, supra, pág. 125.

126 Id. (en donde se afirma que no se admiten las enmiendas a los datos personales para evitar la divulgación).
127 Véase Agencia Española de Protección de Datos, supra.
128 Véase Organización para la Cooperación y el Desarrollo Económicos, supra, art. 13; Ley orgánica, supra, art. 15; Oficina del Comisionado Federal para la Privacidad, supra, pág. 127 (en donde se observa que el controlador de datos no puede desconocer un pedido de acceso a los datos personales porque la persona no haya pagado los cargos pertinentes).
129 Véase también Ley de protección de datos personales de Argentina No. 25.326, § 14, supra; Oficina del Comisionado Federal para la Privacidad, supra, pág. 49.
130 Véase Agencia Española de Protección de Datos, supra.
131 Id.
132 Id.
133 Id.
134 Véase Ley orgánica, supra, art. 16.
135 Véase Agencia Española de Protección de Datos, supra.
136 Véase también id.
137 Id.
138 Id.; Oficina del Comisionado de Información, supra, pág. 137.
139 Véase Oficina del Comisionado de Información, supra, pág. 137.
140 Id.
141 Id. págs. 137 y 138; Agencia Española de Protección de Datos, supra.
142 Véase Agencia Española de Protección de Datos, supra.
143 Id.
144 Véase Ley de protección de datos personales de Argentina No. 25.326, § 14, supra; Oficina del Comisionado de Información, supra, pág. 127.
145 Véase Ley de protección de datos personales de Argentina No. 25.326, § 14, supra.
146 Id.
147 Véase Oficina del Comisionado de Información, supra, pág. 129 y 130.
148 Véase Agencia Española de Protección de Datos, supra.
149 Id.
150 Id.
151 Véase Agencia Española de Protección de Datos, supra; Oficina del Comisionado Federal para la Privacidad, supra, pág. 54.Véase también Organización para la Cooperación y el Desarrollo Económicos, supra, art. 11.
152 Véase Agencia Española de Protección de Datos, supra.
153 Id.; Oficina del Comisionado Federal para la Privacidad, supra, págs. 44 y 45.

154 Oficina del Comisionado Federal para la Privacidad, supra, págs. 45 y 46.
155 Véase Agencia Española de Protección de Datos, supra.
156 Id.
157 Id.
158 Id.
159 Véase Ley de protección de datos personales de Argentina No. 25.326, § 10, supra.
160 Véase Agencia Española de Protección de Datos, supra.
161 Id.
162 Véase Agencia Española de Protección de Datos, supra; Oficina del Comisionado de Información, supra, pág. 14.
163 Id.
164 Véase Agencia Española de Protección de Datos, supra.
165 Véase Ley orgánica, supra, art. 26.
166 Id.
167 Véase Agencia Española de Protección de Datos, supra.
168 Id.
169 Véase Agencia Española de Protección de Datos, supra.
170 Véase Ley orgánica, supra, art. 19.
171 Véase Agencia Española de Protección de Datos, supra.
172 Véase Ley de protección de datos personales de Argentina No. 25.326, § 32, supra; Oficina del Comisionado de Información, supra, págs. 16 y 17.
173 Id.
174 Véase también Agencia Española de Protección de Datos, supra.
175 Id.
176 Véase id.
177 Id.
178 Id.
179 Id.