97º PERÍODO ORDINARIO DE SESIONES
3 – 7 agosto de 2020
Sesión virtual

OEA/Ser. Q
CJI/doc. 616/20 rev.1 corr.1
7 agosto 2020
Original: español/inglés

COMITÉ JURÍDICO INTERAMERICANO (CJI)

PROYECTO DE ACTUALIZACIÓN A LOS "PRINCIPIOS *SOBRE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS PERSONALES, CON ANOTACIONES"*, ADOPTADOS POR EL CJI EN 2015

PARA COMENTARIOS DE LOS ESTADOS MIEMBROS DE LA OEA

Para facilidad de referencia, algunas de las actualizaciones propuestas son seguidas de texto temporal, entre corchetes, que indica la referencia cruzada a disposiciones similares contenidas en otros instrumentos internacionales sobre protección de datos, a saber:

- *Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, adoptados por la Red Iberoamericana de Protección de Datos el 20 de junio de 2017 (en adelante, los "Estándares Iberoamericanos");*
- *El Reglamento General de Protección de Datos de la Unión Europea, en vigor desde el 25 de mayo de 2018 (en adelante, "GDPR" por sus siglas en inglés);*
- *La Ley de Privacidad del Consumidor de California, en vigor desde el 1 de enero de 2020 (en adelante, "CCPA" por sus siglas en inglés).*
- *La Decisión del Secretario-General de la Organización para la Cooperación y Desarrollo Económico (OCDE) sobre la Protección de Individuos en relación con el Procesamiento de sus Datos Personales en vigor desde el 3 de mayo de 2019 (la "Decisión de la OCDE").*
- *Marco de Reglas de Privacidad Transfronteriza del Foro de Cooperación Económica Asia-Pacífico, que implementa el marco de privacidad actualizado en 2015 (en adelante, "APEC CBPR" por sus siglas en inglés).*
- *Tratado México Estados Unidos Canadá, en vigor desde el 1 de julio de 2020 (en lo sucesivo "USMCA" por sus siglas en inglés).*

ACTUALIZACIÓN DE LOS "PRINCIPIOS SOBRE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS PERSONALES, CON ANOTACIONES"

I. LOS PRINCIPIOS

PRINCIPIO UNO
Propósitos Legítimos y Justos

Los datos personales deberían ser recopilados solamente para fines legítimos y por medios justos y legales.

PRINCIPIO DOS
Transparencia y Consentimiento

Antes o en el momento en que se recopilen, se deberían especificar las categorías de datos personales a ser recopiladas, los fines para los cuales se recopilan y usarán los datos personales, los destinatarios o categorías de destinatarios a los cuales los datos personales han sido o serán comunicados, y los derechos del titular en relación con los datos personales a ser recopilados. Cuando el procesamiento se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento de la persona a que se refieran.

PRINCIPIO TRES
Pertinencia y Necesidad

Los datos deberían ser pertinentes y necesarios para los fines expresos de su recopilación.

PRINCIPIO CUATRO
Uso Limitado y Retención

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

PRINCIPIO CINCO
Deber De Confidencialidad

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

PRINCIPIO SEIS
Protección y Seguridad

La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas u organizacionales razonables y adecuadas contra procesamientos no autorizados o ilegítimos y contra la pérdida, destrucción o daños accidentales.

PRINCIPIO SIETE
Exactitud de los Datos

Los datos personales deberían mantenerse exactos, completos, veraces y actualizados hasta donde sea necesario para los propósitos de su uso.

PRINCIPIO OCHO
Acceso, Rectificación, Cancelación, Oposición y Portabilidad

Se debería disponer de métodos razonables para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso, rectificación y cancelación de sus datos, así como el derecho a oponerse a su procesamiento y, en lo aplicable, el derecho a la portabilidad de esos

datos personales. Como regla general, el ejercicio de esos derechos debería ser gratuito. En caso de que fuera necesario restringir los alcances de estos derechos, las bases específicas de cualquier restricción deberían especificarse en la legislación nacional.

PRINCIPIO NUEVE
Datos Personales Sensibles

Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Los controladores de datos deberían adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los individuos titulares de los datos.

PRINCIPIO DIEZ
Responsabilidad

Los controladores de datos deberían adoptar e implementar las medidas técnicas y organizacionales correspondientes para asegurar y poder demostrar que el procesamiento se realiza en conformidad con estos Principios. El controlador y el procesador de datos y, en lo aplicable, sus representantes, deberían cooperar, a petición, con las autoridades de protección de datos personales en el ejercicio de sus tareas.

PRINCIPIO ONCE
Flujo Transfronterizo de Datos y Responsabilidad

Los Estados Miembros deberían cooperar entre sí en la creación de mecanismos y procedimientos que aseguren que los controladores y procesadores de datos que operen en más de una jurisdicción puedan ser efectivamente hechos responsables por el cumplimiento de estos Principios.

PRINCIPIO DOCE
Excepciones

Cuando las autoridades nacionales establezcan excepciones a estos Principios por motivos relacionados con la soberanía nacional, la seguridad nacional, la seguridad pública, la protección de la salud pública, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, la protección de los derechos y libertades de otros o el interés público, deberían establecerlas de manera expresa en una ley o norma y ponerlas en conocimiento del público.

PRINCIPIO TRECE
Autoridades de Protección de Datos

Los Estados Miembros deberían establecer órganos de supervisión independientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de conformidad con estos Principios.

II. LAS ANOTACIONES

Introducción

La finalidad de actualizar los “Principios sobre la Privacidad y la Protección de Datos Personales (con anotaciones)” adoptados por el Comité Jurídico Interamericano (CJI) en 2014 es contribuir al

desarrollo de un marco vigente para salvaguardar los derechos de la persona a la protección de sus datos personales y a la autodeterminación informativa en los países de las Américas. Esta actualización de los Principios se basa en normas y estándares reconocidos a nivel internacional, según han evolucionado hasta el año 2020. Su intención es fortalecer los esfuerzos de los Estados Miembros de la OEA para proteger a las personas de la recopilación, el uso, la retención y la divulgación ilícitos o innecesarios de sus datos personales.

La siguiente explicación detallada de los Principios tiene por objeto proporcionar una guía para la preparación, actualización e implementación de leyes nacionales y normas conexas en los Estados Miembros de la OEA.

Cada Estado Miembro debería determinar cuál es la mejor manera de implementar estos Principios en su ordenamiento jurídico interno. Sea por medio de leyes, normas u otros mecanismos, los Estados Miembros deberían establecer reglas efectivas para la protección de datos personales que den efecto al derecho de la persona a la privacidad y que respeten sus datos personales, protegiendo al mismo tiempo que la persona pueda beneficiarse del libre flujo de información y del acceso a la economía digital.

La finalidad de estos Principios es proporcionar los elementos básicos de una protección efectiva. Los Estados podrían ofrecer mecanismos adicionales para garantizar la privacidad y la protección de los datos personales, teniendo en cuenta las funciones y los propósitos legítimos para los cuales se recopilen y se usen en beneficio de las personas. En general, los Principios reflejan la importancia de la efectividad, la razonabilidad, la proporcionalidad y la flexibilidad como elementos rectores.

Ámbito de aplicación

Estos Principios se aplican a los sectores público y privado por igual, es decir, tanto a los datos personales generados, recopilados o administrados por entidades públicas como a los datos recopilados y procesados por entidades privadas[1]. Se aplican tanto a los datos personales impresos como a los archivos electrónicos. Los Principios no se aplican a los datos personales utilizados por una persona exclusivamente en el contexto de su vida privada, familiar o doméstica. Tampoco se aplican a la información anónima, es decir, aquella que no guarde relación con una persona física identificada o identificable, así como a los datos personales que han sido sujetos a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado (*cf.* definición de 'anonimización', *infra*).

[NOTA: Basado en numeral 4.3 de los Estándares Iberoamericanos.]

Los Principios están relacionados entre sí y deberían interpretarse en conjunto.

El concepto de privacidad

El concepto de privacidad está consagrado en el derecho internacional. Se basa en los conceptos fundamentales del honor personal y la dignidad, así como en la libertad de expresión, pensamiento, opinión y asociación. Hay disposiciones relativas a la protección de la privacidad, el honor personal y la dignidad en los principales sistemas de derechos humanos del mundo.

---

[1] Con respecto al derecho específico de las personas de tener acceso a la información pública, véase la Ley Modelo Interamericana sobre Acceso a la Información Pública, adoptada por la Asamblea General de la OEA el 8 de junio de 2010 mediante la resolución AG/RES. 2607 (XL-O/10), en la cual se incorporan los principios enunciados por la Corte Interamericana de Derechos Humanos en Claude Reyes vs. Chile, Sentencia de 19 de septiembre de 2006 (Serie C No 151), así como los Principios sobre el Derecho de Acceso a la Información, adoptados por el Comité Jurídico Interamericano mediante la resolución CJI/RES. 147 (LXXIII-O/08).

En las Américas, estos conceptos están claramente establecidos en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre (1948) y en los artículos 11 y 13 de la Convención Americana sobre Derechos Humanos ("Pacto de San José") (1969) (apéndice A). La Corte Interamericana de Derechos Humanos ha confirmado el derecho a la privacidad[2].

Además, la constitución y las leyes fundamentales de muchos Estados Miembros de la OEA garantizan el respeto y la protección de datos personales como un derecho distinto y complementario a los derechos a la privacidad, la dignidad personal y el honor familiar, la inviolabilidad del hogar y las comunicaciones privadas y conceptos conexos. Casi todos los Estados Miembros de la OEA han adoptado algún tipo de legislación con respecto a la protección de la privacidad y los datos (aunque sus disposiciones varían en lo que se refiere a su enfoque, ámbito de aplicación y contenido). En consonancia con estos derechos fundamentales, los Principios de la OEA reflejan los conceptos de autodeterminación en lo que respecta a la información, la ausencia de restricciones arbitrarias del acceso a los datos personales, y la protección de la privacidad, la identidad, la dignidad y la reputación.

[Nota: Basado en el párrafo preambular (2) de los Estándares Ibero-Americanos]

Al mismo tiempo, tal como se reconoce en todos los ordenamientos jurídicos, el derecho a la privacidad no es absoluto y puede tener limitaciones razonables relacionadas de manera racional con metas apropiadas.

El concepto del libre flujo de información

Asimismo, los principios fundamentales de la libertad de expresión y de asociación y el libre flujo de información se reconocen en los principales sistemas de derechos humanos del mundo, entre ellos el Sistema Interamericano; por ejemplo, en el artículo IV de la Declaración Americana de los Derechos y Deberes del Hombre (1948) y en el artículo 13 de la Convención Americana (apéndice A). Estos derechos civiles y políticos esenciales se reflejan en las Américas en la constitución y las leyes fundamentales de todos los Estados Miembros de la OEA (aunque cabe reiterar que sus disposiciones varían en cuanto a su enfoque, ámbito de aplicación y contenido). Son cruciales para la promoción de la democracia y las instituciones democráticas.

En una "sociedad de la información" centrada en la persona y orientada al desarrollo, la protección del derecho de las personas a tener acceso a información y conocimientos, a usarlos y a difundirlos puede ayudar a las personas, a las comunidades y a los pueblos a alcanzar su pleno potencial, promover el desarrollo sostenible y mejorar la calidad de vida en general, de acuerdo con los propósitos y principios de la Carta de la OEA y con nuestros instrumentos regionales de derechos humanos.

Definiciones

Anonimización. Tal como se usa en estos Principios, la palabra "anonimización" se refiere a la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.

[NOTA: Basado en el numeral 2.1(a) de los Estándares Iberoamericanos]

Datos personales. Tal como se usa en estos Principios, el término "datos personales" abarca la información que identifica o puede usarse de manera razonable para identificar a una persona física de

[2] "[E]l ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública", Caso de las Masacres de Ituango vs. Colombia, Sentencia de 1 de julio de 2006 (párr. 149), que se encuentra en http://www.corteidh.or.cr/docs/casos/articulos/seriec_148_esp.pdf.

forma directa o indirecta, especialmente por referencia a un número de identificación, datos de localización, un identificador en línea o a uno o más factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social. Incluye información expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otro tipo. El término no abarca la información que no identifica a una persona en particular (o no puede usarse de manera razonable para identificarla).

[NOTA: Basado en el artículo 4.1 del GDPR, el artículo 2.c de los Estándares Iberoamericanos y §1798.140(o)(1) del CCPA]

En los Principios, la palabra "datos" se usa intencionalmente en un sentido amplio a fin de conferir la protección más amplia posible a los derechos de las personas afectadas, independientemente de la forma particular en que se recopilen, se almacenen, se recuperen, se usen o se difundan los datos. En general, en los Principios se evita el uso de la frase "información personal", la cual, por sí sola, podría interpretarse en el sentido de que no incluye "datos" específicos tales como elementos fácticos, "bits" almacenados electrónicamente o registros digitales. Análogamente, la palabra "datos" podría interpretarse en el sentido de que no incluye compilaciones de hechos que, tomados en conjunto, permitan sacar conclusiones sobre la persona o las personas en particular. Por ejemplo, los detalles relativos a la estatura, el peso, el color del cabello y la fecha de nacimiento de dos personas podrían constituir "datos" que, al compararlos, revelen la "información" de que son hermano y hermana o tal vez gemelos idénticos. A fin de promover la mayor protección posible de la privacidad, estos Principios se aplicarían en ambos casos y no permitirían que un controlador de datos efectuara distinciones de ese tipo.

Ejemplos de datos personales incluyen identificadores como el nombre real, alias, dirección postal, identificador personal único, identificador en línea, dirección de protocolo de internet, dirección de correo electrónico, nombre de cuenta, número de seguridad social, número de licencia de conducir, número de pasaporte u otros identificadores similares, o información comercial, información biométrica, información de internet u otra actividad de redes electrónicas (como historial de navegación, historial de búsqueda e información sobre la interacción de un titular con un sitio web, aplicación o anuncio, datos de geolocalización, información de audio, electrónica, visual, termal, olfatoria u otra similar, información profesional o relacionada al trabajo, información educativa e inferencias derivadas de lo anterior para crear un perfil de las preferencias, características, tendencias psicológicas, predisposiciones, comportamiento, actitudes, inteligencia, habilidades y aptitudes del titular de datos, entre otras.

[NOTA: Basado en §1798.140(o))1) del CCPA]

A efectos de estos Principios, solo la gente (personas físicas) tiene intereses en materia de privacidad, a diferencia de los dispositivos, las computadoras o los sistemas mediante los cuales interaccionan. Tampoco tienen intereses en materia de privacidad las organizaciones u otras personas jurídicas con las que tratan. Los menores (personas que no han llegado a la edad adulta) también tienen intereses legítimos en materia de privacidad que deberían reconocerse y protegerse efectivamente en la legislación nacional.

Controlador de datos. Tal como se usa en estos Principios, guía, el término "controlador de datos" significa la persona física o jurídica, entidad privada, autoridad pública u otro organismo u organización o servicio que (solo o junto con otros) se encarga del almacenamiento, el procesamiento, el uso, la protección y la difusión de los datos personales en cuestión. En general abarca las personas físicas o jurídicas o las autoridades facultadas por las leyes nacionales para tomar decisiones con respecto al contenido, el propósito y el uso de un archivo de datos o una base de datos. En algunas circunstancias, este término sería aplicable también a entidades que pueden describirse como "recopiladores de datos", ya que, en la mayoría de los casos, la entidad que almacena, usa y difunde los datos personales también se encarga (de manera directa o indirecta) de recopilarlos.

[NOTA: Basado en el numeral 2.1(g) de los Estándares Iberoamericanos y el artículo 4.7 del GDPR]

Procesador de datos. El término "procesador de datos" se refiere más específicamente a la persona física o jurídica, entidad privada, autoridad pública u otro organismo u organización que (solo o junto con otros) procesa los datos en cuestión. Por lo general y en la gran mayoría de los Estados de la región americana, el procesador de datos es diferente del recopilador de datos y actúa a nombre y por cuenta de éste. En algunos casos, el controlador de datos podría ser también el procesador de datos o podría efectuar arreglos para que otros se ocupen del procesamiento sobre la base de una relación contractual. El término "procesamiento de datos" se usa en un sentido amplio y abarca toda operación o conjunto de operaciones realizado con datos personales, como recopilación, registro, almacenamiento, alteración, recuperación, divulgación o transferencia.

[NOTA: Con base en el numeral 2.1(e) de los Estándares Iberoamericanos y el artículo 4.8 del GDPR]

Autoridad responsable de la protección de datos. Como se utiliza en estos Principios, el término "autoridad responsable de la protección de datos" se refiere a las autoridades supervisoras establecidas en los Estados Miembros, que tienen la facultad de redactar e implementar las leyes, reglamentos y requisitos relacionados con la protección de datos personales, sea a nivel nacional, regional o municipal y de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado.

[NOTA: Basado en el artículo 4.8 del GDPR]

Titular de los datos. Es la persona cuyos datos personales se recopilan, procesan, almacenan, utilizan o difunden.

Datos personales sensibles. El término "datos personales sensibles" se refiere a una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas. Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales o vida sexual, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas o el origen racial o étnico. En ciertas circunstancias podría considerarse que estos datos merecen una protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria.

[NOTA: Con base en el numeral 2.1(d) y 9 de los Estándares Iberoamericanos, en el artículo 9 del GDPR y en el artículo 4.2 de la Decisión de la OCDE]

En los Principios se reconoce que la sensibilidad de los datos personales puede variar según la cultura y cambiar con el tiempo y que los riesgos de ocasionar daños reales a una persona como consecuencia de la divulgación de datos podrían ser insignificantes en una situación en particular pero podrían poner en peligro la vida en otra.

PRINCIPIOS SOBRE PROTECCIÓN DE LA PRIVACIDAD Y LOS DATOS PERSONALES (CON ANOTACIONES)

PRINCIPIO UNO: PROPÓSITOS LEGÍTIMOS Y JUSTOS

Los datos personales deberían ser recopilados solamente para fines legítimos y por medios justos y legales.

Este Principio abarca dos elementos: 1) los "fines legítimos" para los cuales se recopilan inicialmente los datos personales y 2) los "medios justos y legales" con los cuales se efectúa la recopilación inicial.

La premisa es que muchas o incluso la mayoría de las intrusiones en los derechos de las personas pueden evitarse si se respetan los conceptos conexos de legalidad y justicia desde el comienzo, cuando se recopilan inicialmente los datos. Desde luego, estos Principios se aplican y deberían respetarse en todo el proceso de recopilación, compilación, almacenamiento, utilización, divulgación y eliminación de datos personales, no solo en el momento de su recopilación. Sin embargo, es más probable que se cumplan si se recalcan y se respetan desde el comienzo.

Fines legítimos

El requisito de legalidad del fin para el cual se recopilan, retienen y procesan los datos personales es una norma fundamental, profundamente arraigada en valores democráticos básicos y en el estado de derecho. En principio, la recopilación de datos personales debería ser limitada y realizarse con el conocimiento o el consentimiento de la persona. No deberían recopilarse datos sobre personas excepto en las situaciones y con los métodos permitidos o autorizados por ley y (por lo general) deberían darse a conocer a las personas afectadas en el momento en que se recopilen.

Los Estados Miembros deberían, por lo tanto, incluir en sus legislaciones nacionales disposiciones específicas sobre los fines legítimos del procesamiento de datos personales. Como regla general, éstos deberían incluir casos en los que: (a) el titular de los datos otorgue su consentimiento expreso al procesamiento de sus datos personales para uno o varios fines específicos; (b) el procesamiento sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales; (c) el procesamiento sea necesario para el cumplimiento de una obligación legal aplicable al controlador de datos; (d) el procesamiento sea necesario para proteger intereses vitales del titular o de otra persona; (e) el procesamiento sea necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al controlador de datos; (f) el procesamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el controlador de datos o por un tercero; (g) el procesamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente; y (h) el procesamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública.

[NOTA: Basado en el artículo 6.1 de GDPR y el numeral 11.1 de los Estándares Iberoamericanos]

El requisito de legalidad abarca el concepto de legitimidad y excluye la recopilación arbitraria y caprichosa de datos personales. Implica transparencia y una estructura jurídica a la cual pueda tener acceso la persona cuyos datos estén recopilándose.

En la mayoría de los contextos se puede cumplir con el requisito de legalidad si el recopilador o procesador de datos informa al titular de los datos sobre las bases jurídicas de la solicitud de los datos en el momento de su recopilación (por ejemplo, “se solicita su número de identificación personal de conformidad con la Ley de Registro Nacional de 2004” o “la Directiva 33-25 del Ministerio de Economía”).

En otros casos podría necesitarse una explicación diferente, como “se requiere esta información para garantizar que el reembolso se envíe a la dirección correcta del reclamante”. En tales casos, se deberían indicar claramente los fines para los cuales se recopilan los datos, a fin de que la persona pueda entender cómo se recopilarán, usarán o divulgarán los datos.

Medios justos y legales

El Principio Uno también requiere que los medios que se empleen para recopilar datos personales sean “justos y legales”. Los datos personales se recopilan por medios justos y legales cuando la

recopilación es compatible tanto con los requisitos jurídicos pertinentes como con las expectativas razonables de las personas basadas en su relación con el controlador de datos o con otra entidad que recopile los datos y en el aviso o los avisos dados a las personas en el momento en que se recopilen sus datos.

Este Principio excluye la obtención de datos personales por medio de fraude, engaño o con pretextos falsos. Se infringiría, por ejemplo, si una organización se hiciera pasar por otra en llamadas de tele marketing, avisos publicitarios impresos o mensajes por correo electrónico a fin de engañar a los titulares e inducirles a dar el número de su tarjeta de crédito, información sobre cuentas bancarias u otros tipos de información personal delicada.

[NOTA: Basado en el No. 15 de los Estándares Iberoamericanos]

La "justicia" es contextual y depende de las circunstancias. Requiere, entre otras cosas, que se ofrezcan opciones apropiadas a las personas con respecto a la forma y el momento en que vayan a proporcionar datos personales a controladores de datos en los casos en que no sea razonable prever que puedan recopilarse en vista de la relación de las personas con el recopilador o procesador de datos y del aviso o los avisos que hayan recibido en el momento en que se recopilaron sus datos. Las opciones que se ofrezcan a las personas no deberían interferir en las actividades y en la obligación de los controladores de datos de promover la seguridad externa e interna y el cumplimiento de la normativa ni impedir que empleen prácticas comúnmente aceptadas para la recopilación y utilización de datos personales.

Al aplicar estos Principios, los Estados Miembros podrían establecer un requisito de "justicia" separado del tema del engaño.

PRINCIPIO DOS: TRANSPARENCIA Y CONSENTIMIENTO

Antes o en el momento en que se recopilen, se deberían especificar las categorías de datos personales a ser recopiladas, los fines para los cuales se recopilan y usarán los datos personales, los destinatarios o categorías de destinatarios a los cuales los datos personales han sido o serán comunicados, y los derechos del titular en relación con los datos personales a ser recopilados. Cuando el procesamiento se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento de la persona a que se refieran.

[NOTA: Basado en el numeral 12, 16 y 25 de los Estándares Iberoamericanos, el artículo 15 del GDPR y §1798.100(b) y §1798.110(a)(4)y (b)(4) de CCPA]

Este Principio también se centra en la recopilación de datos personales. Se basa en el concepto de la "autodeterminación en lo que respecta a la información" y, en particular, en dos conceptos que gozan de amplio reconocimiento a nivel internacional: el principio de "transparencia" y el principio de "consentimiento". Combinados, estos Principios requieren que (i) se especifiquen las categorías de datos personales a ser recopiladas, los fines para los cuales se recopilen y usen datos personales, así como los destinatarios o categorías de destinatarios a quienes se divulgarán los datos personales y los derechos del titular de datos personales en relación con los datos a ser recopilados, generalmente a más tardar en el momento en el cual se inicie la recopilación; y (ii) cuando el procesamiento se base en el consentimiento, se recopilen datos personales solo con el consentimiento claro de la persona a la que se refieran.

Transparencia

Las categorías de datos personales a ser recopiladas, los fines para los cuales se recopilan y usarán los datos personales, así como los destinatarios o categorías de destinatarios a quienes se divulgarán los datos personales y los derechos del titular de datos personales en relación con los datos a ser recopilados

deberían especificarse claramente antes o en el momento en el cual se recopilen. Además, se debería informar a las personas sobre las prácticas y políticas de las entidades o personas que recopilen los datos personales, a fin de que puedan tomar una decisión fundamentada con respecto al suministro de tales datos. Sin claridad, el consentimiento de la persona con respecto a la recopilación de los datos no puede ser válido.

A fin de que las personas cuenten con fundamentos para decidir a quiénes proporcionarán sus datos personales y por qué razón, se necesita más información que los meros fines de la recopilación, las categorías y el manejo de esos datos. Es importante que se les informe también sobre el fundamento jurídico de la recopilación de sus datos personales, la forma en que se almacenarán y procesarán, la identidad del controlador de esos datos e información para contactarlo, toda transferencia de datos que pueda efectuarse, la existencia, formas y mecanismos o procedimientos de que disponen para ejercer sus derechos de solicitar al controlador de datos el acceso, rectificación o cancelación de sus datos personales o de objetar a su procesamiento, así como su derecho a portabilidad de datos y, cuando los datos personales no hubieren sido recopilados directamente del titular, cualquier información disponible sobre su origen.

[NOTA: Basado en el numeral 16.2 de los Estándares Iberoamericanos, articulo 15 de GDPRy §1798.105(b) y §1798.110 of CCPA]]

La información debería ser proporcionada al titular en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño.

[NOTA: Basado en el artículo 12.1 del GDPR y el numeral 16.3 de los Estándares Iberoamericanos]

Consentimiento

Por lo general, la persona debería ser capaz de dar su consentimiento libremente respecto de la recopilación de datos personales de la forma y con los fines previstos. Por lo tanto, el consentimiento de la persona debería basarse en suficiente información y ser claro, es decir, no debería dar lugar a ninguna duda o ambigüedad con respecto a la intención de la persona. Para que el consentimiento sea válido, la persona debería contar con suficiente información sobre los detalles concretos de los datos que se recopilarán, la forma en que se recopilarán, los fines del procesamiento y toda divulgación que pueda efectuarse. La persona debería ser capaz de efectuar una elección real.

La persona no debería correr ningún riesgo de engaño, intimidación, coacción o consecuencias negativas significativas si se niega a dar el consentimiento.

El método para obtener el consentimiento debería ser apropiado para la edad y la capacidad de la persona afectada (si se conocen) y para las circunstancias particulares del caso. En la obtención del consentimiento de niñas y niños, el controlador de datos debería obtener la autorización del titular de la patria potestad o tutela, conforme a lo dispuesto en las reglas de representación previstas en el derecho interno de los Estados, o en su caso, debería solicitar directamente la autorización del menor de edad si el derecho interno de cada Estado ha establecido una edad mínima para que lo pueda otorgar directamente y sin representación alguna del titular de la patria potestad o tutela.

[NOTA: Basado en el artículo 8 del GDPR y el numeral 13.1 de los Estándares Iberoamericanos]

El consentimiento debería reflejar la preferencia y la decisión fundamentada de la persona afectada. Evidentemente, el consentimiento obtenido bajo coacción o sobre la base de declaraciones falsas o incluso información incompleta o engañosa no puede cumplir las condiciones para la recopilación o el procesamiento legítimos.

[NOTA: Basado en el numeral 12.1 de los Estándares Iberoamericanos]

Contexto

El requisito del consentimiento debería interpretarse de manera razonable en el entorno tecnológico en rápida evolución en el cual se recopilan y usan los datos personales en la actualidad. La índole del consentimiento podría variar según las circunstancias del caso. En estos Principios se reconoce que, en algunas circunstancias, el "conocimiento" podría ser la norma apropiada en los casos en que el procesamiento y la divulgación de datos satisfagan intereses legítimos. El consentimiento implícito podría ser apropiado cuando los datos personales en cuestión son menos sensibles y cuando se proporciona información razonable sobre el propósito y el método de recopilación de manera tal que se cumplan los requisitos de transparencia.

Por ejemplo, el consentimiento de una persona con respecto a la recopilación de algunos datos personales podría inferirse de manera razonable de interacciones anteriores con controladores de datos (y los avisos dados por ellos) y en los casos en que la recopilación sea acorde con el contexto de la transacción para la cual se recopilaron los datos originalmente. También podría inferirse de prácticas comúnmente aceptadas con respecto a la recopilación y el uso de datos personales o las obligaciones legales de los controladores de datos.

En unos pocos casos podría autorizarse la recopilación de algunos datos personales sin consentimiento. En esos casos, la parte que procure recopilar y procesar los datos debería demostrar que tiene una necesidad clara de hacerlo para los fines de sus intereses legítimos o los de un tercero a quien puedan divulgarse los datos. También se debería demostrar que hay un equilibrio entre los intereses legítimos de la parte que busque la divulgación y los intereses del titular de los datos.

La condición de los "intereses legítimos" no se cumplirá si el procesamiento tendrá efectos perjudiciales en los derechos y libertades o en intereses legítimos del titular de los datos. En los casos en que haya una gran discrepancia entre intereses en pugna, los intereses legítimos del titular de los datos tienen prelación. La recopilación y el procesamiento de datos de acuerdo con la condición de los intereses legítimos deberían ser justos y legales y ceñirse a todos los principios de la protección de datos.

Los datos personales sensibles podrían procesarse sin el consentimiento explícito de su titular solo en los casos en que ello sea claramente de gran interés público (según lo que esté autorizado por ley) o responda a intereses vitales del titular de los datos (por ejemplo, en una situación de emergencia en la cual corra peligro su vida).

Momento

Por lo general, se debería informar a la persona sobre los fines en el momento en el cual se recopilen los datos y se debería obtener su consentimiento en ese momento. En la mayoría de los casos, el consentimiento durará todo el tiempo que lleve el procesamiento al cual se refiera. En algunos casos, la recopilación subsiguiente de más datos podría basarse de manera razonable en el consentimiento anterior dado por la persona en relación con la recopilación inicial.

El titular debería tener tiene derecho a retirar su consentimiento en cualquier momento, para lo cual el controlador deberá establecer mecanismos sencillos, ágiles, eficaces y gratuitos. En general, el retiro del consentimiento no afecta la validez del procesamiento que se hubiere hecho sobre la base del consentimiento antes de su retiro.

[NOTA: Basado en el artículo 7.3 del GDPR y el numeral 12.2 de los Estándares Iberoamericanos]

PRINCIPIO TRES: PERTINENCIA Y NECESIDAD

Los datos deberían ser pertinentes y necesarios para los fines expresos de su recopilación.

La pertinencia y la necesidad son principios cruciales de la protección de datos y la privacidad personal. Desde luego, sus requisitos deberían evaluarse en relación con el contexto específico en el cual se recopilen, usen y divulguen los datos. Las consideraciones contextuales incluyen qué datos particulares se recopilan y con qué fines.

Pertinencia

El requisito de que los datos sean "pertinentes" significa que deberían guardar una relación razonable con los fines para los cuales hayan sido recopilados y se tenga la intención de usarlos. Por ejemplo, los datos relativos a opiniones podrían ser fácilmente engañosos si se usan para fines con los cuales no guarden ninguna relación.

Necesidad y proporcionalidad

Por lo general, los procesadores de datos deberían usar datos personales solamente de una forma acorde con los fines expresos de la recopilación; por ejemplo, cuando sean necesarios para proporcionar el servicio o el producto solicitado por la persona. Asimismo, los recopiladores y procesadores de datos deberían seguir un criterio de "limitación" o "minimización", de acuerdo con el cual deberían hacer un esfuerzo razonable para cerciorarse de que los datos personales que manejen correspondan al mínimo requerido para el fin expreso. En algunos sistemas jurídicos se usa el concepto de "proporcionalidad" para hacer referencia al equilibrio de valores en pugna. La proporcionalidad requiere que las instancias decisorias determinen si una medida ha ido más allá de lo que se requiere para alcanzar una meta legítima y si los beneficios alegados excederán los costos previstos.

[NOTA: Basado en el artículo 5.1(c) de GDPR]

En el contexto del procesamiento de datos del sector público, la idea de necesidad a veces se mide sobre la base de la proporcionalidad; por ejemplo, al exigir un equilibrio entre 1) el interés del público en el procesamiento de los datos personales y 2) la protección de los intereses de las personas en materia de privacidad.

De acuerdo con estos Principios, los conceptos de "necesidad" y "proporcionalidad" imponen limitaciones generales al uso, lo cual significa que los datos personales solo deberían usarse para cumplir los propósitos de la recopilación excepto con el consentimiento de la persona cuyos datos personales se recopilen o cuando sea necesario para proporcionar un producto o servicio solicitado por la persona.

No obstante, en los Principios se reconoce que el campo de la gestión y el procesamiento de datos están evolucionando continuamente desde el punto de vista tecnológico. En consecuencia, debería entenderse que este Principio abarca una medida razonable de flexibilidad y adaptabilidad.

PRINCIPIO CUATRO: USO LIMITADO Y RETENCIÓN

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

En este Principio se enuncian dos premisas fundamentales con respecto a la retención de datos personales: 1) deberían mantenerse y utilizarse de una manera legítima que no sea incompatible con el fin para el cual se hayan recopilado (lo cual se denomina a veces el "principio de finalidad" o "limitación del propósito") y 2) no deberían mantenerse más tiempo del necesario para su propósito y de conformidad con la legislación nacional correspondiente.

Uso limitado

Con respecto a la primera premisa, los datos personales deberían manejarse con propósitos determinados, específicos, explícitos y legítimos. La retención y el uso de datos personales deberían ser compatibles con las expectativas razonables de las personas, su relación con el controlador que recopile los datos y el aviso o los avisos proporcionados por el controlador de datos.

[NOTA: Basado en el artículo 5.1(b) del GDPR y el numeral 17.1 de los Estándares Iberoamericanos]

No deberían mantenerse ni utilizarse datos personales con fines que no sean compatibles con aquellos para los cuales se hayan recopilado, excepto con el conocimiento o consentimiento del titular de los datos o por mandato de la ley. El concepto de "incompatibilidad" da cierto grado de flexibilidad, ya que permite hacer referencia al objetivo o propósito general en relación con el cual la persona haya dado inicialmente su consentimiento para que se recopilaran datos. En ese sentido, la medida apropiada suele consistir en respetar el contexto en el cual la persona haya proporcionado sus datos personales y las expectativas razonables de la persona en esa situación particular.

[NOTA: Basado en §1798.100(b) de CCPA]

Por ejemplo, cuando un titular da su nombre y su dirección a un vendedor en línea y dicho vendedor, a su vez da el nombre del titular y su domicilio particular al expedidor para que se puedan entregar al comprador los productos comprados, esa divulgación es evidentemente un uso "compatible" de datos personales. Sin embargo, si el vendedor da el nombre del titular y su domicilio particular a otro tipo de vendedor o comerciante con fines que no sean necesarios para completar la transacción en línea del titular y que no estén relacionados con dicha transacción, lo más probable es que sea un uso "incompatible" de los datos del consumidor y que no esté permitido salvo que el titular dé su consentimiento expreso.

El procesamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

[NOTA: Basado en el numeral 17.3 de los Estándares Iberoamericanos, articulo 5.1(b) de GDPR y§1798.140(o)(3)(s) de CCPA]

Así, otro caso en el cual este Principio podría aplicarse de manera razonable y con un alto grado de flexibilidades el uso de los datos personales de una persona como parte de un procesamiento más amplio (o "agregado") de datos de un gran número de personas por el controlador de datos; por ejemplo, para la elaboración de inventarios o con fines estadísticos o de contabilidad.

Retención limitada

Los datos personales deberían mantenerse de forma que se permita la identificación de los interesados únicamente durante el tiempo que sea necesario para los fines del procesamiento de los datos personales. La realidad de la tecnología moderna exige una limitación general para la retención de datos. Como el costo del almacenamiento de datos ha bajado considerablemente, suele ser menos costoso para los controladores de datos almacenar datos indefinidamente en vez de examinarlos y borrar los que no

sean necesarios. No obstante, la retención innecesaria y excesiva de datos personales evidentemente tiene implicaciones para la privacidad. Como regla general, por lo tanto, los controladores deberían disponer de manera segura y definitiva de los datos -a través, por ejemplo, de eliminarlos de los archivos, registros, bases de datos, expedientes o sistemas de información de los controladores, o bien deberían someterlos a un proceso de anonimización, cuando ya no se necesiten para su fin original o tal como se disponga en la legislación nacional.

[NOTA: Basado en el artículo 5.1(d) del GDPR y numeral 19.2 y 19.3 de los Estándares Iberoamericanos]

Los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas a fin de proteger los derechos y libertades del titular.

[NOTA: Basado en el artículo 5.1(e) de GDPR]

Asimismo, las personas pueden optar por consentir, ya sea de forma expresa o por implicación, en que se usen y retengan sus datos personales con fines adicionales. La legislación interna pertinente impone requisitos legales explícitos para la retención de datos. Asimismo, un controlador de datos podría tener razones legales legítimas para retener datos durante un período determinado aunque eso no se requiera explícitamente. Por ejemplo, los empleadores podrían conservar expedientes de ex empleados o los médicos podrían conservar expedientes de ex pacientes a fin de protegerse de ciertos tipos de acción judicial, como juicios por mal ejercicio de la profesión, despido ilegal, etc. Podría ser necesario que los controladores de datos retengan datos personales durante períodos más largos a fin de cumplir otras obligaciones legales o proteger los derechos, la seguridad o los bienes de la persona, del procesador de datos o de un tercero.

[NOTA: Basado en el numeral 19.4 de los Estándares Iberoamericanos].

PRINCIPIO CINCO: DEBER DE CONFIDENCIALIDAD

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

Este Principio deriva del deber básico del controlador de datos de mantener la "confidencialidad" de los datos personales en un entorno seguro y controlado.

Este deber requiere que el controlador de datos se cerciore de que no se proporcionen tales datos (ni se pongan a disposición por otros medios) a personas o entidades excepto con el conocimiento o consentimiento de la persona afectada, en consonancia con las expectativas razonables de la persona afectada o por mandato de la ley. El controlador de datos debería cerciorarse también de que los datos personales no se usen con fines que sean incompatibles con el fin original para el cual se recopilaron los datos. Estas responsabilidades emanan de la naturaleza misma de los datos personales y no dependen de afirmaciones de las personas afectadas.

[NOTA: Basado en el numeral 23 de los Estándares Iberoamericanos]

Este deber de respetar los límites de la divulgación se suma a la obligación de los controladores de datos enunciada en el Principio Seis de promover la seguridad externa e interna y el cumplimiento de la normativa al salvaguardar los datos. Proteger la privacidad implica no solo mantener la seguridad de los datos personales, sino también permitir que las personas controlen la forma en que se usan y divulgan sus datos personales. Un elemento esencial de la "autodeterminación en lo que respecta a la información" es el establecimiento y mantenimiento de la confianza entre el titular de los datos y el controlador de datos, especialmente con respecto a la divulgación de datos personales a terceros.

En algunos casos sería razonable inferir el consentimiento de la persona del contexto particular de su relación e interacciones con el controlador de datos o sus servicios, el aviso o los avisos dados por el controlador de datos y las prácticas aceptadas comúnmente para la recopilación y el uso de datos personales. Por ejemplo, en algunos casos sería enteramente razonable que un controlador de datos proporcionara datos a un tercero "proveedor de servicios" (por ejemplo, un procesador de datos) en el marco de un arreglo contractual especificado.

La divulgación a agentes de las fuerzas del orden y a otros organismos gubernamentales de conformidad con la legislación no contravendría este Principio, pero debería autorizarse por medio de disposiciones claras y específicas.

La protección de los datos personales en poder de las autoridades públicas puede estar sujeta a normas diferentes en función de la naturaleza de la información y las razones de la divulgación. Estas razones y normas también deberían ser tratadas por disposiciones claras y específicas. En este contexto, se llama la atención a la Ley Modelo Interamericana sobre Acceso a la Información Pública, aprobada en 2010, así como al proyecto de Ley Modelo 2.0 que aprobó el CJI en 2020 y actualmente discuten los órganos políticos de la OEA, conforme al cual los sujetos obligados deben proteger a la información confidencial de las personas y en particular, los datos personales cuya divulgación requiera autorización de sus titulares.

PRINCIPIO SEIS: PROTECCIÓN Y SEGURIDAD

La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas u organizacionales razonables y adecuadas contra procesamientos no autorizados o ilegítimos y contra la pérdida, destrucción o daños accidentales.

De acuerdo con este Principio, los controladores de datos deberían establecer y mantener las medidas de carácter administrativo y técnicas que sean necesarias para establecer salvaguardias de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos personales que obren en su poder o bajo su custodia (o de los cuales sean responsables) y cerciorarse de que tales datos personales no sean procesados ni divulgados excepto con el conocimiento o consentimiento de la persona o de otra autoridad legítima, ni que sean accidentalmente perdidos, destruidos o dañados.

[NOTA: Basado en el artículo 5.1(f) de GDPR y el numeral 21.1 y 23.1 de los Estándares Iberoamericanos]

Los controladores de datos deberían proporcionar "salvaguardias razonables y adecuadas". Se basa en la consecución y el mantenimiento de un nivel apropiado de atención en el contexto de la situación general. Por lo tanto, hay que tener en cuenta consideraciones de proporcionalidad y necesidad.

En el contexto moderno, es técnicamente imposible garantizar la privacidad absoluta y la protección completa de los datos personales, y el esfuerzo necesario para lograrlo impondría barreras indeseables y costos inaceptables. Asimismo, es posible que en distintos contextos se requieran soluciones y niveles de salvaguardias diferentes. Por consiguiente, este Principio requiere un juicio razonado y fundamentado y no se viola necesariamente cada vez que un controlador de datos experimente un acceso no autorizado, pérdida, destrucción, daño, uso, modificación o divulgación.

Los datos personales deberían protegerse, independientemente de la forma en que se mantengan, por medio de salvaguardias razonablemente concebidas para prevenir que las personas sufran daños considerables como consecuencia del acceso no autorizado a los datos o de su pérdida o destrucción. La índole de las salvaguardias podría variar según la sensibilidad de los datos en cuestión.

Evidentemente, para los datos más sensibles se requiere un nivel más alto de protección. Algunas de las razones para conferir mayor protección podrían ser, por ejemplo, los riesgos de usurpación de la identidad, pérdidas económicas, efectos negativos en la calificación crediticia, daños a bienes y pérdida del empleo o de oportunidades comerciales o profesionales.

La norma no es estática. Las amenazas a la privacidad, especialmente las amenazas cibernéticas, están evolucionando constantemente y la determinación de lo que constituye salvaguardias "razonables y adecuadas" debería responder a esa evolución. El reto consiste en proporcionar orientación válida a los controladores de datos, procurando al mismo tiempo que las normas sigan siendo "tecnológicamente neutrales" y no se vuelvan obsoletas como consecuencia de los rápidos cambios tecnológicos.

En vista de la celeridad de los cambios en el entorno actual de la información, una práctica que hace solo unos meses era permisible podría considerarse en la actualidad como una práctica intrusiva, riesgosa o peligrosa para la privacidad individual. Análogamente, una restricción que haya parecido razonable hace algunos meses podría ser obsoleta o injusta a la luz de los adelantos tecnológicos.

Por lo tanto, la determinación relativa a la existencia de "salvaguardias razonables y adecuadas" debería basarse en los métodos y técnicas más avanzados que estén en uso en el ámbito de la seguridad de los datos en vista de la evolución de las amenazas a la privacidad personal. Asimismo, debería reverse, evaluarse y mejorarse periódicamente.

[NOTA: Basado en el numeral 21.3 de los Estándares Iberoamericanos]

La protección de la privacidad de las personas implica mantener la seguridad de sus datos personales y permitir que las personas controlen su experiencia "en línea". Además de tomar medidas de seguridad eficaces, los controladores de datos (tales como los proveedores de servicios en línea) deberían tener flexibilidad para proporcionar a sus usuarios medios efectivos para controlar el intercambio de datos personales como parte de las medidas generales de protección de la privacidad.

Violaciones de los datos personales

La incidencia creciente de intrusiones externas ("violaciones de los datos personales"), que consisten en el acceso no autorizado a datos protegidos, suscita preocupaciones relacionadas con la privacidad y con el ámbito penal. En muchos países, entre los cuales se cuentan Estados Miembros de la OEA, la notificación es obligatoria por ley en esos casos. Por consiguiente, en caso de violación de los datos, los controladores de datos podrían tener la obligación legal de notificar a las personas cuyos datos hayan sido (o puedan haber sido) comprometidos.

Tales notificaciones permiten a las personas afectadas tomar medidas de protección y posiblemente tener acceso a los datos y pedir que se corrijan datos inexactos o el uso indebido de los datos como consecuencia de su violación. Las notificaciones también podrían ofrecer incentivos a los controladores de datos para asumir la responsabilidad, examinar las políticas en materia de retención de datos y mejorar sus medidas de seguridad.

Al mismo tiempo, las leyes sobre notificación de violaciones de datos podrían imponer a los controladores de datos la obligación de cooperar con las fuerzas del orden en el ámbito penal y con otras autoridades (por ejemplo, equipos de respuesta a incidentes de informática u otras entidades responsables de la supervisión de la ciber seguridad). En la legislación nacional se deberían indicar las (pocas) situaciones concretas en que las fuerzas del orden puedan requerir la divulgación de datos personales sin el consentimiento de las personas afectadas. Hay que tener cuidado de no imponer requisitos contradictorios a los controladores de datos con respecto a la notificación y la confidencialidad.

En los casos en que se imponen sanciones a los controladores de datos por incumplimiento del deber de salvaguardar y proteger, tales sanciones deberían ser proporcionales al grado de perjuicio o de riesgo. En este contexto podría ser útil que las jurisdicciones nacionales adoptaran definiciones específicas de lo que constituye una "violación" (o "acceso no autorizado"), los tipos de datos que podrían requerir un grado mayor de protección en esos casos y las responsabilidades específicas que podría tener un controlador de datos en caso de una divulgación de ese tipo.

PRINCIPIO SIETE: EXACTITUD DE LOS DATOS

Los datos personales deberían mantenerse exactos, completos, veraces y actualizados hasta donde sea necesario para los propósitos de su uso.

La exactitud y la precisión revisten una importancia vital para la protección de la privacidad. Evidentemente, la exactitud de los datos es importante para la protección de la privacidad. Los datos inexactos pueden perjudicar tanto al procesador de datos como al titular de los datos, pero en una medida que varía mucho según el contexto.

Cuando se recopilan datos personales y se los retiene para seguir usándolos (en vez de usarlos una sola vez o durante períodos cortos), el controlador de datos tiene la obligación de tomar medidas para que los datos en su posesión se mantengan actualizados y sean exactos y completos, de tal manera que no se altere la veracidad de éstos conforme se requiera para los fines para los cuales se hayan recopilado y se usen.

[NOTA: Basado en el numeral 19.1 de los Estándares Iberoamericanos]

Podría o no ser necesario actualizar continuamente los datos y velar siempre para que estén completos a fin de que sean exactos en lo que se refiere al fin expreso para el cual se hayan recopilado. Para decidir si se necesita más información, se debería aplicar la norma de la "necesidad", es decir que los datos en cuestión deberían ser exactos y completos y estar actualizados al grado necesario para los propósitos para los que serán usados. Esta obligación deriva del "uso" para el cual se hayan recopilado los datos y del uso que se haya dado o se tenga la intención de dar a los datos y en relación con el cual la persona haya dado su consentimiento. No es un requisito abstracto de exactitud objetiva. Por lo tanto, el controlador o los controladores de datos deberían adoptar mecanismos apropiados, que sean razonables a la luz del fin para el cual se hayan recopilado los datos y con el cual se usen, a fin de que los datos sigan siendo veraces, exactos, completos, correctos y actualizados y que no se menoscaben los derechos de la persona en cuestión.

Los controladores de datos deberían tomar medidas efectivas para salvaguardar la privacidad de las personas y de otros que proporcionen sus propios datos. A fin de cumplir sus obligaciones con respecto a la exactitud, deberían dar a las personas una oportunidad razonable para examinar o corregir la información personal que hayan suministrado al controlador de datos o para solicitar que se la borre. Se podría establecer un plazo razonable para la vigencia de este requisito.

Al tomar medidas para determinar la exactitud de los datos personales de una persona ("calidad de los datos"), el controlador de datos podría considerar la sensibilidad de los datos personales que recopile o mantenga y la probabilidad de que expongan a las personas a daños considerables, de conformidad con los requisitos del Principio Nueve.

Como se mencionó bajo los Principios Tres y Cuatro, bajo los criterios de 'minimización' y uso limitado y retención, los datos personales que se procesen deberían corresponder al mínimo requerido para los fines especificados y no debería retenerse por más del tiempo que sea necesario para tales fines.

En muchos casos, para aplicar este Principio será necesario borrar datos personales que ya no se necesiten para los fines que justificaron inicialmente su recopilación.

En ciertas circunstancias (por ejemplo, para la investigación de fraudes o la protección contra fraudes) podría ser necesario que los procesadores de datos necesiten retener y procesar algunos datos inexactos o fraudulentos.

[NOTA: Basado en el numeral 19.3 de los Estándares Iberoamericanos]

PRINCIPIO OCHO: ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN Y PORTABILIDAD

Se debería disponer de métodos razonables para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso, rectificación y cancelación de sus datos, así como el derecho a oponerse a su procesamiento y, en lo aplicable, el derecho a la portabilidad de esos datos personales. Como regla general, el ejercicio de esos derechos debería ser gratuito. En caso de que fuera necesario restringir los alcances de estos derechos, las bases específicas de cualquier restricción deberían especificarse en la legislación nacional.

[NOTA: Basado en el Capítulo III de los Estándares Iberoamericanos]

Las personas deberían tener derecho a saber si los controladores de datos tienen datos personales relacionados con ellas. Deben tener acceso a esos datos a fin de que puedan impugnar su exactitud y pedir al controlador de datos que modifique, revise, corrija o elimine los datos en cuestión. Este derecho de acceso y rectificación es una de las salvaguardias más importantes en el campo de la protección de la privacidad. Deben también tener derecho a cancelar sus datos personales y a objetar su procesamiento. Cuando sea aplicable, tienen también derecho a la portabilidad de sus datos.

Los elementos esenciales son la capacidad de la persona para obtener datos relacionados con ella en un plazo razonable y de una forma razonable e inteligible; para saber si se ha denegado una solicitud de acceso a dichos datos y por qué; y para impugnar tal denegación. Como regla general, el ejercicio de esos derechos debería ser gratuito; excepcionalmente, los costos deberían ser solamente aquellos asociados por razones naturales de reproducción, envió o certificación de los datos.

[NOTA: Basado en el párrafo preambular 19 de los Estándares Ibero-Americanos; párrafo 1798.100(d) de CCPA]

En el ordenamiento jurídico interno de algunos países de las Américas (pero no en todos) se reconoce el derecho de *habeas data*, en virtud del cual las personas pueden entablar juicio para prevenir un presunto abuso de sus datos personales o ponerle fin. Ese derecho podría dar a la persona acceso a bases de datos públicas o privadas, así como el derecho a corregir los datos en cuestión, a mantener el carácter confidencial de los datos personales sensibles y a rectificar o borrar datos perjudiciales. Como el contorno específico de este derecho varía de un Estado Miembro a otro, en estos Principios se abordan las cuestiones que plantea desde el punto de vista de cada uno de sus elementos.

La legislación nacional de cada Estado debería establecer los requerimientos, plazos, términos y condiciones en que los titulares podrán ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad, así como las causales de improcedencia al ejercicio de los mismos. Estos derechos no son absolutos, y las legislaciones nacionales deberían especificar claramente las causas y razones por las cuales puede ser improcedente su ejercicio. Tales causales podrían incluir, de manera enunciativa mas no limitativa: 1) cuando el procesamiento sea necesario para el cumplimiento de un objetivo importante de interés público o para el ejercicio de las funciones propias de las autoridades públicas; 2) cuando el controlador acredite tener motivos legítimos para que el procesamiento prevalezca sobre los intereses, los derechos y las libertades del titular; 3) cuando el procesamiento sea necesario

para el cumplimiento de una disposición legal; o 4) cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

En caso de fallecimiento o desaparición del titular, la legislación nacional de cada Estado podrá reconocer que las personas físicas que sean sus familiares o representantes legales ejerzan los derechos a que se refieren estos Principios respecto de los datos personales de esas personas.

Además, la legislación nacional de cada Estado podrá reconocer el derecho que tiene el titular de inconformarse o impugnar las respuestas otorgadas por el controlador, o bien su falta de respuesta, ante una solicitud de ejercicio de los derechos aludidos en el presente Principio, ante la autoridad de control y, en su caso, ante instancias judiciales de conformidad con el derecho interno de cada Estado.

[NOTA: Basado en los numerales 32.3 y 32.4 de los Estándares Iberoamericanos]

Los controladores y procesadores de datos no deberían discriminar contra los titulares en razón de que éstos hubieren ejercido cualquiera de estos derechos, incluyendo de manera enunciativa mas no limitativa mediante la denegación de bienes o servicios al titular, la cobranza de precios o tarifas diferentes por ellos o el otorgamiento de un nivel o calidad distinta de los bienes.

[NOTA: Basado en §1798.125 de CCPA]

El derecho de acceso

El derecho de acceso a los datos personales mantenidos por un controlador de datos debería ser sencillo de ejercer. Por ejemplo, los mecanismos de acceso deberían formar parte de las actividades regulares del controlador de datos y no se debería requerir ninguna medida especial o procedimiento judicial (como la presentación formal de un reclamo por la vía judicial). Cada persona debería tener la posibilidad de tener acceso a sus propios datos. En algunos casos, hasta terceros podrían tener derecho también (por ejemplo, los representantes de personas con discapacidad mental o los padres de menores).

La capacidad de una persona para tener acceso a sus datos se conoce también como derecho de "participación individual". De acuerdo con este concepto, se debería otorgar acceso dentro de un plazo razonable de una manera razonable y en una forma razonablemente inteligible. Según se mencionó, el acceso debería otorgarse libre de costo; excepcionalmente, los costos deberían ser solamente los asociados por razones naturales de reproducción, envío y certificación de los datos. La carga y el costo de la presentación de los datos no deberían ser irrazonables o desproporcionados.

[NOTA: Basado en el párrafo preambular 19 de los Estándares Iberoamericanos y el párrafo 1798.100(d) de CCPA]

Todo dato que vaya a proporcionarse a su titular debería presentarse de una forma inteligible, usando un lenguaje claro y sencillo. La información debería entregarse por correo o de manera electrónica, y en caso de otorgarse de manera electrónica debería ser portable según lo especificado más adelante (cf. sección 'Derecho a la portabilidad de datos', *infra*).

[NOTA: Basado en el párrafo preambular 19 y 25 de los Estándares Iberoamericanos; el artículo 15 del GDPR; el párrafo 1798.100(d) de CCPA]

Excepciones y limitaciones

Sin embargo, el derecho de acceso no es absoluto. En todo sistema nacional hay situaciones excepcionales en las cuales se podría requerir que se mantenga el carácter confidencial de ciertos datos. Estas circunstancias deberían enunciarse claramente en las leyes apropiadas o en otras directrices y deberían ponerse a disposición del público.

Por ejemplo, podrían surgir situaciones de ese tipo si se sospecha que la persona a la cual se refieren los datos ha cometido un acto ilícito y es el sujeto de una investigación que estén realizando las fuerzas del orden o una entidad similar, si los registros de esa persona están mezclados con los de un tercero que también tiene intereses en materia de privacidad o si otorgar acceso al titular de los datos podría comprometer secretos comerciales, pruebas confidenciales o material para exámenes. Las reglas relativas a situaciones de esos tipos deberían ser lo más estrechas y restrictivas posible.

Además, por razones prácticas, un controlador de datos podría imponer condiciones razonables; por ejemplo, especificando el método para efectuar solicitudes y exigiendo que las personas que efectúen solicitudes de ese tipo autentiquen su identidad por medios razonables. No es necesario que los controladores de datos accedan a solicitudes que impongan cargas o gastos desproporcionados, que violen los derechos a la privacidad de otras personas, que infrinjan datos reservados o secretos comerciales, que contravengan las obligaciones legales de los controladores de datos o que impidan de cualquier otra forma que la compañía proteja los derechos, la seguridad o los bienes de la compañía, de otro usuario, de una filial o de un tercero.

El derecho a impugnar la denegación de acceso

Si a una persona se le deniega la solicitud de acceso, debería haber un método efectivo para que la persona (o su representante) pueda averiguar las razones de la denegación e impugnarla. Es necesario permitir que la persona se entere de las razones de una decisión adversa a fin de que pueda ejercer el derecho a impugnar la decisión y prevenir la denegación arbitraria.

Como ya se dijo, en algunos casos bien podría ser apropiado, o incluso necesario, retener ciertos datos. Sin embargo, esos casos deberían ser la excepción y no la regla, y las razones de la denegación deberían comunicarse claramente a la persona que efectúe la solicitud, a fin de prevenir la denegación arbitraria del derecho fundamental a corregir errores.

El derecho de rectificación para corregir errores y omisiones

La persona debería tener la posibilidad de ejercer el derecho a solicitar la corrección (o la adición) de datos personales sobre sí misma que sean incompletos, inexactos, innecesarios, excesivos o no se encuentren actualizados. Eso se conoce también como derecho de “rectificación.” Si los datos en cuestión son incompletos o inexactos, se debería permitir que la persona proporcione más información a fin de corregir los errores u omisiones.

Si los datos en cuestión son evidentemente inexactos, el controlador de datos por lo general debería corregir la inexactitud cuando el titular de los datos lo solicite. Incluso en los casos en que se determine que los datos son inexactos, como en el curso de una investigación del titular de los datos, a veces podría ser más apropiado que el controlador de datos agregue material al registro en vez de borrarlo, a fin de que refleje con exactitud la historia completa de la investigación.

No se debería permitir que el titular de los datos introduzca datos inexactos o erróneos en los registros del controlador de datos. El titular de los datos tampoco tiene necesariamente derecho a compeler al controlador de datos a que borre datos que sean exactos pero embarazosos.

El derecho de corrección o rectificación no es absoluto. Por ejemplo, es posible que no se autorice la modificación de datos personales, aunque se trate de información errónea o engañosa, en los casos en que los datos se requieran legalmente o deban ser retenidos para el cumplimiento de una obligación

impuesta a la persona responsable por la ley nacional pertinente o posiblemente por las relaciones contractuales entre la persona responsable y el titular de los datos.

Por consiguiente, en la legislación nacional se deberían indicar claramente las condiciones en las cuales se debería proporcionar acceso y permitir la corrección de los datos, así como las restricciones que se apliquen. Se deberían especificar las situaciones limitadas en las cuales no se pueda tener acceso a datos personales y no exista la posibilidad de corregirlos. Se deberían especificar claramente los motivos de tales restricciones.

Derecho a la cancelación

En algunos marcos reglamentarios nacionales y regionales se da a las personas el derecho a solicitar que los controladores de datos supriman (o borren) datos personales específicos respecto de los cuales, aunque estén a disposición del público, las personas afirmen que ya no son necesarios o pertinentes o el titular retire su consentimiento o se oponga a su procesamiento. Este derecho se describe a veces como el derecho a omitir o suprimir información específica, es decir, como derecho a la "desidentificación" o a la "anonimización". Donde se reconoce el derecho a la cancelación, y ante una solicitud en ese sentido, los controladores de datos deberían proceder a suprimir los datos personales de sus registros y deberían también ordenar a cualquier procesador de datos que elimine los datos personales de sus registros.

[NOTA: basado en el art. 17 de GDPR, No. 27 de los Estándares Iberoamericanos y §1798.105 de CCPA]

Este derecho no es absoluto sino contingente y contextual, y requiere un equilibrio difícil de intereses y principios. El ejercicio del derecho plantea necesariamente cuestiones fundamentales en lo que se refiere no solo a la privacidad, el honor y la dignidad, sino también al derecho de acceso a la verdad, la libertad de información y de expresión, y la proporcionalidad. Las excepciones al ejercicio del derecho de cancelación deberían estar específicamente establecidas en las legislaciones domésticas, y pueden incluir, por ejemplo, casos en los cuales los datos son necesarios para completar la transacción para la cual se recopilaron los datos, cumplir los términos de una garantía escrita o una devolución de producto realizada conforme a la ley, ejecutar un contrato, detectar incidentes de seguridad, proteger contra actividad maliciosa, engañosa, fraudulenta o ilegal, depurar para identificar y reparar errores, ejercer la libertad de expresión o llevar a cabo investigación científica, histórica o estadística de interés público, entre otros.

[NOTA: basado en §1798.105 de CCPA]

En algunos Estados, el "derecho a borrar o suprimir" sigue siendo controvertido y es el tema de definiciones y puntos de vista divergentes, en relación con datos personales que (aunque sean ciertos o exactos en cuanto a los hechos) la persona afectada considere personalmente embarazosos, excesivos o simplemente irrelevantes.

El derecho de oposición

El titular debería tener el derecho de oponerse, en razón de su situación particular, en cualquier momento al procesamiento de sus datos personales cuando tenga una razón legítima para ello o cuando el procesamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad. Cuando el titular se oponga al procesamiento con fines de mercadotecnia directa, sus datos personales dejaran de ser tratados para dichos fines.

[NOTA: Basado en el artículo 21 de GDPR y No. 28 de los Estándares Iberoamericanos]

El derecho a la portabilidad de sus datos personales

Cuando se procesen datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al controlador en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro controlador sin impedimento, en caso de que lo requiera.

[NOTA: Basado en el párrafo preambular 19 de los Estándares Iberoamericanos; artículo 20 de GDPR; párrafo 1798.100(d) de CCPA]

El titular podrá solicitar que sus datos personales se transfieran directamente de controlador a controlador, cuando sea técnicamente posible. El derecho a la portabilidad de los datos personales no afectará negativamente los derechos y libertades de otros.

Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no debería resultar procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o procesamiento efectuado por el controlador con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

[NOTA: basado en el artículo 30.4 de los Estándares Iberoamericanos y el artículo 20 de GDPR]

PRINCIPIO NUEVE: DATOS PERSONALES SENSIBLES

Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Los controladores de datos deberían adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los individuos titulares de los datos.

El término "datos personales sensibles" abarca los datos que se refieren a los aspectos más íntimos de las personas. Según el contexto cultural, social o político, podría incluir, por ejemplo, los datos relacionados con su salud personal, vida sexual, preferencias sexuales, creencias religiosas, filosóficas o morales, afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera univoca a una persona física, opinión política u origen racial o étnico.

[NOTA: Con base en el numeral 2.1(d) de los Estándares Iberoamericanos, el artículo 9 de GDPR y articulo 4.2 de la Decisión de OCDE]

Estos datos merecen protección especial porque, si se manejan o se divulgan de manera indebida, darían lugar a una intrusión profunda en la dignidad personal y el honor de la persona afectada y podrían desencadenar una discriminación ilícita o arbitraria contra la persona o causar un riesgo de graves perjuicios para la persona.

Por consiguiente, deberían establecerse garantías apropiadas en el contexto de la legislación y la normativa nacionales a fin de proteger en medida suficiente los intereses de las personas en materia de privacidad. Los Estados Miembros deberían indicar claramente las categorías de datos personales que se consideren especialmente "sensibles" y que, por consiguiente, requieran una mayor protección, así como el alcance de la prohibición de su procesamiento y las excepciones a la misma. Como regla general, los datos personales sensibles no deberían ser procesados excepto, por ejemplo, cuando el titular ha otorgado consentimiento explícito para ello o cuando el procesamiento es estrictamente necesario para el ejercicio y cumplimiento de las atribuciones y obligaciones específicas del controlador de datos, o es necesario para dar cumplimiento a un mandato legal, o es necesario por razones de seguridad nacional, seguridad

pública, orden público, salud pública, o salvaguarda de derechos y libertades de terceros. Al determinar las obligaciones reglamentarias pertinentes, hay que tener en cuenta el contexto en el cual una persona proporciona esos datos.

[NOTA: Basado en el No. 9 de los Estándares Iberoamericanos y el artículo 9 de GDPR]

Debe recaer en los controladores de datos la carga de determinar los riesgos importantes para los titulares de los datos como parte del proceso general de gestión de riesgos y evaluación del impacto en la privacidad. Si se responsabiliza a los controladores de datos, se podrá proteger mejor a los titulares de los datos contra daños considerables en una amplia gama de contextos culturales.

[NOTA: Basado en el No. 9 de los Estándares Iberoamericanos]

PRINCIPIO DIEZ: RESPONSABILIDAD

Los controladores de datos deberían adoptar e implementar las medidas técnicas y organizacionales correspondientes para asegurar y poder demostrar que el procesamiento se realiza en conformidad con estos Principios. El controlador y el procesador de datos y, en lo aplicable, sus representantes, cooperarán, a petición, con las autoridades de protección de datos personales en el ejercicio de sus tareas.

[NOTA: Con base en el numeral 20.1 de los Estándares Iberoamericanos y los artículos 24 y 31 de GDPR]

La protección efectiva de los derechos individuales de protección de la privacidad y de los datos se basa tanto en la conducta responsable de los controladores de datos como en las personas y en las autoridades gubernamentales del caso. Los sistemas de protección de la privacidad deberían reflejar un equilibrio apropiado entre la reglamentación gubernamental y la implementación efectiva por aquellos que tienen responsabilidad directa por la recopilación, el uso, la retención y la difusión de datos personales.

Estos Principios dependen de la capacidad de quienes recopilan, procesan y retienen datos personales para tomar decisiones responsables, éticas y disciplinadas acerca de los datos y su uso durante todo el "ciclo de vida" de los datos. Estos "gerentes de datos" deberían actuar en calidad de "buen custodio" de los datos que les proporcionen o confíen.

Responsabilidad

El principio de responsabilidad requiere el establecimiento de metas apropiadas en lo que se refiere a la protección de la privacidad, a las cuales los controladores de datos (organizaciones y otras entidades) deberían adherirse, permitiéndoles determinar las medidas más apropiadas para alcanzar esas metas y vigilar su cumplimiento. De esa forma, los controladores de datos pueden alcanzar las metas en materia de protección de la privacidad de la forma que mejor se adapte a sus modelos empresariales, la tecnología y los requisitos de sus clientes.

Los controladores de datos deberían implementar las medidas organizacionales y técnicas necesarias para asegurar y poder demostrar, a petición, que el procesamiento se realiza de conformidad con estos Principios. Cuando el procesamiento se realiza en nombre de un controlador, el controlador debería usar solo procesadores que otorguen suficientes garantías de implementar medidas técnicas u organizacionales de tal forma que el procesamiento cumpla con estos Principios y asegure la protección de los derechos del titular.

[NOTA: Basado en los artículos 24 y 28 de GDPR y No. 20 de los Estándares Iberoamericanos, y articulo 6.1 de la Decisión de la OCDE]

En los programas y procedimientos se deberían tener en cuenta la índole de los datos personales en cuestión, el tamaño y la complejidad de la organización que recopila, almacena y procesa datos, y el riesgo de violaciones. La protección de la privacidad depende de una evaluación creíble de los riesgos que el uso de datos personales podría plantear para las personas y la mitigación responsable de esos riesgos. Deberían destinarse recursos apropiados para implementar programas, políticas y procedimientos de protección de datos personales, que deberían incluir, entre otros, sistemas de manejo de riesgos, capacitación sobre obligaciones de protección de datos, revisión periódica de programas de seguridad, un sistema de supervisión y vigilancia, incluyendo auditorías, para revisar el cumplimiento de las políticas de protección de datos, así como procedimientos para recibir y responder preguntas y quejas de titulares. La adhesión a códigos de conducta o mecanismos de certificación, entre otros, pueden usarse como elementos para demostrar cumplimiento con estos Principios.

[NOTA: Basado en No. 20.1 a 20.3 de los Estándares Iberoamericanos y articulo 24 de GDPR].

Por lo tanto, las leyes y normas nacionales en materia de privacidad deberían proporcionar una orientación claramente expresada y bien definida a los controladores de datos. Deberían impulsar la elaboración de códigos de conducta autónomos que se mantengan a la par de los adelantos tecnológicos y que tengan en cuenta los principios y normas de privacidad vigentes en otras jurisdicciones.

Los controladores de datos deberían cerciorarse de que los empleados que manejen datos personales estén debidamente capacitados en lo que se refiere a la finalidad de la protección de los datos y los procedimientos que se emplean para protegerlos. Deben adoptar programas efectivos de gestión de la privacidad y realizar revisiones internas con el propósito de promover la privacidad de las personas. En muchos casos, la designación de un "responsable principal de la información y la privacidad" facilitará la consecución de esta meta.

En primer lugar, en las leyes nacionales sobre privacidad se debería exigir que los controladores de datos rindan cuenta del cumplimiento de estos Principios. Además del mecanismo con que cuenten las autoridades gubernamentales para hacer cumplir la normativa, el derecho interno debería proveer a las personas de mecanismos apropiados para responsabilizar a los controladores de datos de las violaciones que se produzcan (por ejemplo, mediante la indemnización por daños y perjuicios).

Incorporación de la privacidad en el diseño de sistemas

Un enfoque contemporáneo eficaz consiste en requerir que los controladores de datos incorporen la protección de la privacidad en el diseño y la arquitectura de sus sistemas de tecnología de la información y en sus prácticas comerciales. Deben incorporarse consideraciones de privacidad y seguridad en cada etapa del diseño de los productos.

Los controladores de datos deberían estar preparados para demostrar sus programas de gestión de la privacidad cuando se lo solicite, en particular a petición de una autoridad de protección de datos personales competente o de otra entidad que se encargue de promover la adhesión a un código de conducta.

[NOTA: Basado en No. 20 de los Estándares Iberoamericanos, artículos 24 y 31 de GDPR y articulo 6.1 de la Decisión de OECD]

Intercambio de datos con terceros

El intercambio y la retransmisión de datos, que están difundiéndose entre los controladores de datos, plantean algunas cuestiones difíciles. Como mínimo, no obstante, el consentimiento de una persona respecto de la recopilación inicial de datos personales no autoriza automáticamente el

intercambio (o la retransmisión) de esos datos con otros controladores o procesadores de datos. Se debería informar a las personas sobre esos intercambios adicionales y ofrecerles oportunidades apropiadas para que den su consentimiento.

Estos Principios indican que los controladores de datos deberían asumir la responsabilidad de asegurar que sus requisitos sean observados por terceros a quienes se comuniquen los datos personales. Esta obligación de asegurar que haya salvaguardias adecuadas de seguridad se aplica independientemente de que otra persona esté a cargo o de que un controlador de datos diferente maneje datos personales en representación de la autoridad responsable (es decir, la que está obligada a rendir cuentas). También se aplica en el caso de transferencias internacionales o transfronterizas de datos personales (véase el Principio Once).

PRINCIPIO ONCE: FLUJO TRANSFRONTERIZO DE DATOS Y RESPONSABILIDAD

Los Estados Miembros deberían cooperar entre sí en la creación de mecanismos y procedimientos que aseguren que los controladores y procesadores de datos que operen en más de una jurisdicción puedan ser efectivamente hechos responsables por el cumplimiento de estos Principios.

En el mundo moderno de rápidos flujos de datos y comercio transfronterizo, es cada vez más probable que las transferencias de datos personales crucen fronteras nacionales. Sin embargo, la reglamentación que existe actualmente en diversas jurisdicciones nacionales varía en cuanto al fondo y al procedimiento. En consecuencia, existe la posibilidad de confusión, conflictos y contradicciones.

Un reto fundamental para una política y una práctica eficaces en materia de protección de datos consiste en conciliar 1) las diferencias en los enfoques nacionales de la protección de la privacidad con la realidad moderna del flujo mundial de datos; 2) los derechos de las personas a tener acceso a datos en un contexto transnacional; y 3) el hecho fundamental de que los datos y el procesamiento de datos impulsan el desarrollo y la innovación. Todos los instrumentos internacionales para la protección de datos procuran alcanzar un equilibrio apropiado entre esas metas.

En estos Principios se expresa una norma común para evaluar los mecanismos de protección de la privacidad en los Estados Miembros de la OEA. La meta fundamental es armonizar los enfoques reguladores que proporcionan una protección más efectiva de la privacidad, al mismo tiempo que se promueven los flujos de datos seguros para el crecimiento económico y el desarrollo. De hecho, no todos los Estados Miembros de la OEA ofrecen en la actualidad exactamente los mismos tipos de protección.

Al igual que en otras normas internacionales en este campo, en estos Principios se adopta una norma de razonabilidad con respecto a las transferencias transfronterizas. Por una parte, deberían permitirse las transferencias internacionales de datos personales entre Estados Miembros que confieran los grados de protección reflejados en estos Principios o que protejan los datos personales en medida suficiente por otros medios, entre ellos mecanismos efectivos de aplicación de la normativa. Al mismo tiempo, deberían permitirse las transferencias también en los casos en que los controladores de datos mismos tomen medidas apropiadas para asegurar que los datos transferidos estén protegidos de manera efectiva en consonancia en estos Principios. Los Estados Miembros deberían tomar las medidas necesarias para que los controladores y procesadores de datos se responsabilicen de esa protección.

Flujo transfronterizo de datos

La transferencia de datos personales a través de fronteras nacionales es un hecho de la vida contemporánea. Nuestra comunidad mundial está más interconectada que nunca. En la mayoría de los

países, cualquiera que tenga un teclado y conexión a internet puede conseguir fácilmente información de todas partes del mundo. En el derecho internacional se reconoce el derecho de las personas a la privacidad y a la protección de datos personales en consonancia con el libre flujo de información. Algo igualmente importante es que las economías nacionales dependen en medida creciente del intercambio y el comercio transfronterizos, y la transferencia de datos (incluidos datos personales) es un aspecto fundamental de ese intercambio y comercio.

Con el surgimiento de nuevas tecnologías, el almacenamiento de datos está volviéndose geográficamente indeterminado. La computación y el almacenamiento "en nube" y la prevalencia creciente de servicios móviles implican necesariamente el intercambio y el almacenamiento remoto de datos a través de fronteras nacionales. Un enfoque progresista de la privacidad y la seguridad debería permitir que las empresas e industrias nacionales crezcan y compitan en el plano internacional. Las restricciones nacionales innecesarias o irrazonables a los flujos transfronterizos de datos podrían crear barreras para el comercio de servicios y dificultar el desarrollo de productos y servicios innovadores, eficientes y eficaces en función del costo. Pueden convertirse fácilmente en obstáculos para las exportaciones y ocasionar perjuicios considerables tanto a los proveedores de servicios como a personas y a clientes empresariales. Las restricciones al flujo transfronterizo de datos personales deberían ser proporcionales a los riesgos presentados, tomando en cuenta la sensibilidad de los datos, y el propósito y contexto del procesamiento. Cualesquier restricciones deberían ser no-discriminatorias.

Se alienta a los Estados Miembros de la OEA a considerar el reconocimiento de estándares interoperables para transferencias transfronterizas a fin de facilitar el flujo irrestricto de datos personales entre Estados Miembros con distintos alcances y estados de desarrollo en sus legislaciones nacionales relativas a la privacidad y protección de datos personales. Esto permitiría responsabilidades compartidas y cooperación entre Estados Miembros en caso de transferencias no autorizadas, y contribuiría a incrementar el comercio, la inversión y los resultados económicos para los Estados Miembros, así como incentivar la innovación y reducir las barreras de entrada a la economía global.

[NOTA: Basado en APEC CBPR y, USMCA art. 19.3]

Restricciones nacionales basadas en distintos grados de protección

En la OEA, todos los Estados Miembros comparten la meta general de proteger la privacidad y un compromiso con el libre flujo de información en el marco de ciertos criterios. Los Estados Miembros deberían abstenerse de restringir el flujo de datos a otros Estados que sustancialmente están observando estos Principios, o donde existen las salvaguardias apropiadas. Lo mismo ocurre con la mayoría de los países del resto del mundo. No obstante, en algunos países las autoridades han impuesto restricciones a la comunicación transfronteriza de datos por personas y entidades sujetas a su jurisdicción en los casos en que, en opinión de esas autoridades, las normas en materia de protección de datos de los otros países no se ciñen a los requisitos específicos de las leyes vigentes en su jurisdicción. Por ejemplo, se podría impedir que una entidad del país A comunique datos a una entidad el país B si, en opinión de las autoridades de A, las leyes de B sobre privacidad o protección de datos no se ciñen a las normas de A, incluso si ambas entidades forman parte de la misma organización comercial.

En (unas pocas) circunstancias particulares, las leyes nacionales podrían restringir justificadamente el flujo transnacional de datos y requerir que los datos se almacenen y procesen localmente. Las razones para restringir o prevenir los flujos de datos deberían ser siempre imperiosas. Algunas razones de tales restricciones podrían ser más imperiosas que otras. No obstante, por lo general los requisitos relativos a la "localización de datos" son en sí contraproducentes y deberían evitarse, prefiriéndose en cambio las medidas de cooperación.

Cooperación internacional

Por estas razones, los principios y mecanismos de la cooperación internacional deberían tratar de limitar y reducir las fricciones y los conflictos entre los distintos enfoques jurídicos internos que rigen el uso y la transferencia de datos personales. El respeto mutuo de los requisitos establecidos en la normativa de otros países (incluidas sus salvaguardias de la privacidad) fomentará el comercio transfronterizo de servicios. Ese respeto, a su vez, debería basarse en un concepto de transparencia entre los Estados Miembros con respecto a los requisitos y los procedimientos para la protección de datos personales.

Los Estados Miembros deberían procurar el reconocimiento mutuo de las reglas y prácticas en materia de responsabilización, a fin de evitar conflictos y resolverlos cuando surjan. Los Estados Miembros deberían promover la transferencia transfronteriza de datos (con las debidas salvaguardias) y no deberían imponer cargas que limiten el libre flujo de información o actividad económica entre jurisdicciones, como exigir que los proveedores de servicios operen en el país o instalen su infraestructura o sus datos dentro de las fronteras de un país. Las leyes nacionales no deberían entorpecer el acceso de los controladores de datos o las personas a la información que esté almacenada fuera del país siempre que la información reciba un grado de protección que se apegue a los estándares aquí descritos.

Responsabilización de los controladores de datos

Desde luego, se debería exigir que los controladores de datos cumplan las obligaciones legales de la jurisdicción donde tengan su domicilio social y donde operen.

Al mismo tiempo, los controladores de datos que transfieran datos personales a través de fronteras deberían asumir la responsabilidad de asegurar un grado continuo de protección que sea acorde con estos Principios.

Los controladores de datos deberían tomar medidas razonables para que los datos personales estén protegidos eficazmente de acuerdo con estos Principios, sea que los datos se transfieran a terceros dentro del país o a través de fronteras internacionales. Asimismo, deberían proporcionar a las personas del caso un aviso apropiado de tales transferencias, especificando los fines para los cuales esos terceros usarán sus datos personales. En general, estas obligaciones deberían reconocerse en acuerdos apropiados, en disposiciones contractuales o por medio de salvaguardias técnicas e institucionales de la seguridad, procesos para la tramitación de quejas, auditorías y medias similares. La idea es facilitar el flujo necesario de datos personales entre Estados Miembros y, al mismo tiempo, garantizar el derecho fundamental de las personas a la protección de sus datos personales.

Estos Principios podrían servir de marco acordado para la cooperación y el fortalecimiento de las capacidades de las autoridades de los Estados Miembros de la OEA encargadas de aplicar la normativa en materia de privacidad, sobre la base de normas comunes para asegurar que se cumplan los requisitos básicos de la responsabilización transfronteriza.

PRINCIPIO DOCE: EXCEPCIONES

Cuando las autoridades nacionales establezcan excepciones a estos Principios por motivos relacionados con la soberanía nacional, la seguridad nacional, la seguridad pública, la protección de la salud pública, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, la protección de los derechos y libertades de otros o el interés público, deberían establecerlas de manera expresa en una ley o norma y ponerlas en conocimiento del público.

[NOTA: Basado en numeral 6 de los Estándares Iberoamericanos y el artículo 23 de GDPR]

Proteger los intereses en materia de privacidad de las personas (los ciudadanos y otros) es cada vez más importante en un mundo donde se recopilan ampliamente datos sobre personas, se los difunde con rapidez y se los almacena durante mucho tiempo. La finalidad de estos Principios es conferir a las personas los derechos básicos que necesitan para salvaguardar sus intereses.

Sin embargo, la privacidad no es el único interés que los Estados Miembros y sus gobiernos deberían tener en cuenta en el campo de la recopilación, retención y difusión de datos. De vez en cuando surgirá inevitablemente la necesidad de tener en cuenta otras responsabilidades del Estado, lo cual llevará a la limitación de los derechos de privacidad de las personas.

En algunos casos, es posible que las autoridades de los Estados Miembros de la OEA tengan que apartarse de estos Principios o establecer excepciones por razones relacionadas con preocupaciones imperiosas de la seguridad nacional y la seguridad pública, la protección de la salud pública, la administración de justicia, el cumplimiento de la normativa u otras prerrogativas esenciales de la política pública u objetivos de interés público general. Por ejemplo, al responder a las amenazas planteadas por la delincuencia internacional, el terrorismo y la corrupción, así como a ciertas violaciones severas a los derechos humanos, las autoridades competentes de los Estados Miembros de la OEA ya han efectuado arreglos especiales para la cooperación internacional en la detección, investigación, sanción y prevención de delitos penales.

[NOTA: Basado en Nº6 de los Estándares Iberoamericanos y articulo 23 de GDPR]

Estas excepciones y desviaciones respecto de la norma deberían ser la excepción y no la regla. Deberían aplicarse solo después de considerar lo más cuidadosamente posible la importancia de proteger la privacidad individual, la dignidad y el honor. Debería haber límites sensatos en la capacidad de las autoridades nacionales para compeler a los controladores de datos a dar a conocer datos personales, manteniendo un equilibrio entre la necesidad de los datos en circunstancias limitadas y el debido derecho de los intereses de las personas en materia de privacidad.

Por medio de leyes o normas públicas, los Estados Miembros deberían indicar claramente esas excepciones y desviaciones respecto de la norma, los casos concretos en que pueda requerirse que los controladores de datos divulguen datos personales y las razones correspondientes. Deberían permitir que los controladores de datos publiquen información estadística pertinente de manera agregada (por ejemplo, el número y la índole de las solicitudes de datos personales efectuadas por el gobierno) como parte del esfuerzo general para promover la protección efectiva de la privacidad. Asimismo, deberían divulgar estos datos al público con prontitud.

PRINCIPIO TRECE:
AUTORIDADES DE PROTECCIÓN DE DATOS

Los Estados Miembros deberían establecer órganos de supervisión independientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de conformidad con estos Principios.

La mayoría de los Estados Miembros de la OEA han establecido organismos reguladores nacionales autónomos que se encargan de establecer y hacer cumplir leyes, normas y requisitos relativos a la protección de datos personales a fin de mantener la uniformidad en todo el país. En otros Estados Miembros se han establecido normas y autoridades en materia de protección de datos en distintos niveles del gobierno (nacional, regional y municipal). En otros, los sistemas de reglamentación difieren según el

sector o la esfera de actividad (bancaria, médica, educacional, etc.) y la responsabilidad podría estar distribuida entre organismos reguladores y entidades privadas con responsabilidades legales específicas.

Como no se observa un enfoque uniforme en la región, cada Estado Miembro de la OEA debería abordar individualmente la naturaleza específica, la estructura, las autoridades y las responsabilidades de estas "autoridades responsables de la protección de datos".

Se insta a los Estados Miembros a que establezcan disposiciones, procedimientos o instituciones jurídicos, administrativos y de otros tipos que sean apropiados y eficaces para proteger la privacidad y las libertades individuales con respecto a los datos personales. Deberían crear medios razonables para que las personas ejerzan sus derechos y fomentar y apoyar la autorregulación (con códigos de conducta o por otros medios) de los controladores de datos y los procesadores de datos. Asimismo, deberían establecer sanciones y recursos adecuados para los casos de incumplimiento y cerciorarse de que no se discrimine injustamente contra los titulares de los datos.

Los Estados Miembros deberían establecer también los requisitos mínimos para cualquier tipo de protección de datos que las autoridades escojan, a fin de proporcionarles los recursos, el financiamiento y la pericia técnica que necesiten para desempeñar sus funciones eficazmente.

ANEXO

Parte I. Derecho a la privacidad

Como se indica en el texto, hay disposiciones relativas a la privacidad, la protección del honor personal y la dignidad, la libertad de expresión y de asociación, y el libre flujo de información en los principales sistemas de derechos humanos del mundo.

Por ejemplo, el concepto de privacidad está claramente establecido en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre (1948) y en el artículo 11 de la Convención Americana sobre Derechos Humanos ("Pacto de San José") (1969)[3].

El artículo V de la Declaración Americana de los Derechos y Deberes del Hombre dispone lo siguiente:

> Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.
>
> Véanse también el artículo IX ("Toda persona tiene el derecho a la inviolabilidad de su domicilio") y el artículo X ("Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia").

El artículo 11 de la Convención Americana sobre Derechos Humanos dispone lo siguiente:

> 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
> 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques[4].

Carta de la Unión Europea

Solamente en la Carta de los Derechos Fundamentales de la Unión Europea (adoptada en 2000) se aborda la privacidad específicamente en el contexto de la protección de datos.

El artículo 8 de la Carta dispone lo siguiente:

> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento

---

3. Véanse también la Declaración Universal de Derechos Humanos (art. 12, 18-20), el Pacto Internacional de Derechos Civiles y Políticos (art. 17-19), el Convenio para la protección de los derechos humanos y de las libertades fundamentales (art. 8-10), la Carta de los Derechos Fundamentales de la Unión Europea (art. 1, 7, 8, 10-12) y la Carta Africana sobre los Derechos Humanos y de los Pueblos (art. 5, 8-11 y 28).

4. Además, el artículo 14 de la Convención Americana ("Derecho de Rectificación o Respuesta") dispone lo siguiente:

> 1. Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.
> 2. En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.
> 3. Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial.

legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Por consiguiente, en la Carta de la Unión Europa al parecer se hace una distinción entre la protección de datos y el derecho al respeto de la vida privada y familiar (art. 7), la libertad de pensamiento, de conciencia y de religión (art. 10), y la libertad de expresión y de información (art. 11). Los expertos siguen debatiendo si existe un derecho independiente a la protección de la información personal o si debería considerarse en cambio como parte de un derecho más general a la privacidad[5/].

Parte II. El derecho al libre flujo de información

El artículo IV de la Declaración Americana de los Derechos y Deberes del Hombre dispone lo siguiente:

Toda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento por cualquier medio.

El artículo 13 de la Convención Americana sobre Derechos Humanos dispone lo siguiente:

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deberían estar expresamente fijadas por la ley y ser necesarias para asegurar:
    a) el respeto a los derechos o a la reputación de los demás, o
    b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.
3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.
4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.
5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

El artículo 19 de la Declaración Universal de Derechos Humanos (1948) dispone lo siguiente:

Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir

---

5. Véase, por ejemplo, Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order", 63 Int'l & Comp. Law Q. 569 (2014).

> informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

El artículo 10 del Convenio para la protección de los derechos humanos y de las libertades fundamentales (titulado "Libertad de expresión") dispone lo siguiente:

> 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.
>
> 2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial.

En la Declaración de Principios de la Cumbre Mundial sobre la Sociedad de la Información, de 2003 (párrs. 24-26) (que se encuentra en: *http://www.itu.int/wsis/docs/geneva/official/dop-es.html)* se recalca lo siguiente:

> La capacidad universal de acceder y contribuir a la información, las ideas y el conocimiento es un elemento indispensable en una Sociedad de la Información integradora.
>
> Es posible promover el intercambio y el fortalecimiento de los conocimientos mundiales en favor del desarrollo si se eliminan los obstáculos que impiden un acceso equitativo a la información para actividades económicas, sociales, políticas, sanitarias, culturales, educativas y científicas, y si se facilita el acceso a la información que está en el dominio público, lo que incluye el diseño universal y la utilización de tecnologías auxiliares.
>
> Un dominio público rico es un factor esencial del crecimiento de la Sociedad de la Información, ya que genera ventajas múltiples tales como un público instruido, nuevos empleos, innovación, oportunidades comerciales y el avance de las ciencias. La información del dominio público debería ser fácilmente accesible en apoyo de la Sociedad de la Información, y debería estar protegida de toda apropiación indebida. Habría que fortalecer las instituciones públicas tales como bibliotecas y archivos, museos, colecciones culturales y otros puntos de acceso comunitario, para promover la preservación de las constancias documentales y el acceso libre y equitativo a la información.

Parte III. Apéndices sobre la privacidad y la protección de los datos

A continuación, se presenta una selección de los textos que más probablemente sean útiles para los legisladores y otras autoridades gubernamentales.

- Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (1980, revisión de 2013)

- La Resolución de Madrid: Estándares Internacionales sobre Protección de Datos Personales y Privacidad (2009)
- Marco de Privacidad de APEC (2004)
- Sistema de Reglas de Privacidad Transfronteriza de APEC
- Directiva 2002/58/EC del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas (12 de julio de 2002)
- Directiva 95/46/EC del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (24 de octubre de 1995)
- Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Nº 108, 28 de enero de 1981) y su Protocolo (2001)
- Principios rectores de las Naciones Unidas para la reglamentación de los ficheros computadorizados de datos personales (1990)
- Convenio de la Unión Africana sobre Ciber seguridad y Datos Personales (adoptado el 27 de junio de 2014)

* * *