Principios Actualizados sobre la Privacidad y la Protección de Datos Personales

OEA

Más derechos para más gente

Carta de la Organización de los Estados Americanos
Capítulo XIV
El Comité Jurídico Interamericano

Artículo 99

El Comité Jurídico Interamericano tiene como finalidad servir de cuerpo consultivo de la Organización en asuntos jurídicos; promover el desarrollo progresivo y la codificación del derecho internacional, y estudiar los problemas jurídicos referentes a la integración de los países en desarrollo del Continente y la posibilidad de uniformar sus legislaciones en cuanto parezca conveniente.

Artículo 100

El Comité Jurídico Interamericano emprenderá los estudios y trabajos preparatorios que le encomienden la Asamblea General, la Reunión de Consulta de Ministros de Relaciones Exteriores o los consejos de la Organización. Además, puede realizar, a iniciativa propia, los que considere conveniente, y sugerir la celebración de conferencias jurídicas especializadas.

Artículo 101

El Comité Jurídico Interamericano estará integrado por once juristas nacionales de los Estados miembros, elegidos por un período de cuatro años, de ternas presentadas por dichos Estados. La Asamblea General hará la elección mediante un régimen que tenga en cuenta la renovación parcial y procure, en lo posible, una equitativa representación geográfica. En el Comité no podrá haber más de un miembro de la misma nacionalidad.

Las vacantes producidas por causas distintas de la expiración normal de los mandatos de los miembros del Comité, se llenarán por el Consejo Permanente de la Organización siguiendo los mismos criterios establecidos en el párrafo anterior.

Artículo 102

El Comité Jurídico Interamericano representa al conjunto de los Estados miembros de la Organización, y tiene la más amplia autonomía técnica.

Artículo 103

El Comité Jurídico Interamericano establecerá relaciones de cooperación con las universidades, institutos y otros centros docentes, así como con las comisiones y entidades nacionales e internacionales dedicadas al estudio, investigación, enseñanza o divulgación de los asuntos jurídicos de interés internacional.

Artículo 104

El Comité Jurídico Interamericano redactará su estatuto, el cual será sometido a la aprobación de la Asamblea General.

El Comité adoptará su propio reglamento.

Artículo 105

El Comité Jurídico Interamericano tendrá su sede en la ciudad de Río de Janeiro, pero en casos especiales podrá celebrar reuniones en cualquier otro lugar que oportunamente se designe, previa consulta con el Estado miembro correspondiente.

Principios Actualizados sobre la Privacidad y la Protección de Datos Personales

Organización de los Estados Americanos
Departamento de Derecho Internacional
Secretaría de Asuntos Jurídicos

OAS Cataloging-in-Publication Data

Organization of American States. Secretariat for Legal Affairs. Department of International Law.

Principios actualizados sobre la privacidad y la protección de datos personales / [Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos].
v. ; cm. (OAS. Documentos oficiales ; OEA/Ser.D/XIX.20)
ISBN 978-0-8270-7414-9
1. Privacy, Right of--America. 2. Data protection--Law and legislation--America. I. Title. II. Inter-American Juridical Committee. III. Series.

OEA/Ser.D/XIX.20

Índice

Presentación

El Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos (OEA) se complace en presentar esta publicación que pone a disposición del público los *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales* adoptados por el Comité Jurídico Interamericano (CJI) y aprobados por la Asamblea General de la OEA en 2021[1].

Estos 13 Principios reflejan las distintas aproximaciones que prevalecen en los Estados miembros sobre los temas centrales de la protección de los datos personales, entre ellos el consentimiento, las finalidades y medios para la captación y tratamiento de estos datos, el flujo transfronterizo y la seguridad de los datos personales, la protección especial a los datos sensibles, y el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

Como una herramienta adicional, esta publicación incluye las anotaciones que explican, ejemplifican y profundizan en los conceptos que constituyen el contenido de cada uno de los Principios Actualizados.

Con la aprobación de los Principios Actualizados se da cumplimiento a un mandato conferido al CJI en junio de 2018 por el órgano máximo de la OEA,

[1] Adoptados mediante la resolución AG/RES. 2974 (LI-O/21) de fecha 11 de noviembre de 2021.

la Asamblea General, consistente en iniciar "la actualización de los Principios sobre la Protección de Datos Personales, teniendo en cuenta la evolución de los mismos".

Así pues, el CJI, mediante la relatoría a cargo de la Dra. Mariana Salazar Albornoz, y con el apoyo del Departamento de Derecho Internacional como Secretaría Técnica, considerando que los Principios sobre Privacidad y Protección de Datos en las Américas habían sido adoptados originalmente por el CJI en 2012, se dio a la tarea de desarrollar un amplio proceso de consultas sobre temas puntuales que deberían ser fortalecidos, revisados o adaptados a la evolución tecnológica y normativa del tratamiento y la protección de los datos personales.

En dicho proceso participaron no solamente Estados Miembros de la OEA, sino también actores como el Comité Internacional de la Cruz Roja, la Comisión Interamericana de Mujeres y la Red Iberoamericana de Protección de Datos, todos ellos aportando valiosos insumos y perspectivas que han sido incorporados al trabajo que aquí presentamos. Adicionalmente, la relatoría tomó en cuenta instrumentos internacionales sobre la protección de datos personales que consagran lo más avanzado en la materia, buscando su plena sintonía con los Principios Actualizados.

De esta manera, los *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*, como instrumento de *soft law* interamericano tienen por objetivo servir a los Estados miembros como punto de referencia para el fortalecimiento de sus respectivos marcos jurídicos en la materia, y orientar el desarrollo colectivo de la región hacia una protección armónica y efectiva de los datos personales.

Dante Negro
Director, Departamento de Derecho Internacional
Secretaría Técnica del Comité Jurídico Interamericano

Parte I
Los Principios

Principio **uno**

Finalidades Legítimas y Lealtad

Los datos personales deberían ser recopilados solamente para finalidades legítimas y por medios leales y legítimos.

Principio **dos**

Transparencia y Consentimiento

Antes o en el momento en que se recopilen, se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para las cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados. Cuando el tratamiento se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento previo, inequívoco, libre e informado de la persona a que se refieran.

Principio **tres**

Pertinencia y Necesidad

Los datos personales deberían ser únicamente los que resulten adecuados, pertinentes, y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior.

Principio **cuatro**

Tratamiento y Conservación Limitados

Los datos personales deberían ser tratados y conservados solamente de manera legítima no incompatible con las finalidades para las cuales se recopilaron. Su conservación no debería exceder del tiempo necesario para cumplir dichas finalidades y de conformidad con la legislación nacional correspondiente.

Principio **cinco**

Confidencialidad

Los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley.

Principio **seis**

Seguridad de los Datos

La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aún cuando éstos ocurran de manera accidental. Dichas salvaguardias deberían ser objeto de auditoría y actualización permanente.

Principio **siete**

Exactitud de los Datos

Los datos personales deberían mantenerse exactos, completos y actualizados hasta donde sea necesario para las finalidades de su tratamiento, de tal manera que no se altere su veracidad.

Principio **ocho**

Acceso, Rectificación, Cancelación, Oposición y Portabilidad

Se debería disponer de métodos razonables, ágiles, sencillos y eficaces 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 tratamiento 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 y estar en conformidad con los estándares internacionales aplicables.

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. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos.

Principio **diez**

Responsabilidad

Los responsables y encargados del tratamiento de datos deberían adoptar e implementar medidas técnicas y organizacionales que sean apropiadas y efectivas para asegurar y poder demostrar que el tratamiento se realiza en conformidad con estos Principios. Dichas medidas deberían ser auditadas y actualizadas periódicamente. El responsable o encargado del tratamiento 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

Reconociendo su valor para el desarrollo económico y social, los Estados Miembros deberían cooperar entre sí para facilitar el flujo transfronterizo de datos personales a otros Estados cuando éstos confieran un nivel adecuado de protección de los datos de conformidad con estos Principios. Asimismo, los Estados Miembros deberían cooperar en la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o los transmitan a una jurisdicción distinta de la suya, puedan garantizar y ser efectivamente hechos responsables por el cumplimiento de estos Principios.

Principio **doce**

Excepciones

Cualquier excepción a alguno de estos Principios debería estar prevista de manera expresa y específica en la legislación nacional, ser puesta en conocimiento del público y limitarse únicamente a 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, o el interés público.

Principio **trece**

Autoridades de Protección de Datos

Los Estados Miembros deberían establecer órganos de supervisión independientes, dotados de recursos suficientes, 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. Los Estados Miembros deberían promover la cooperación entre tales órganos.

Parte 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 2015 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 en lo que respecta a la información 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 proteger a las personas de la recopilación, el uso, la retención y la divulgación ilícitos o innecesarios de Datos Personales.

La siguiente explicación detallada de los Principios tiene por objeto proporcionar una guía para orientar la reflexión al interior de cada Estado Miembro de la OEA ("Estado Miembro") sobre el estado que guarda su normativa en la materia, así como, en su caso, los esfuerzos de fortalecimiento de la misma.

Cada Estado Miembro debería determinar cuál es la mejor manera de tomar en cuenta 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 las finalidades legítimas para su Tratamiento 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 tanto a los sectores público como privado, es decir, tanto a los Datos Personales generados, recopilados o administrados por entidades públicas como a los Datos recopilados y tratados por entidades privadas[1]. Se aplican a los Datos Personales que se encuentren en cualquier soporte físico o digital.

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 seudonimizados o sujetos a un proceso de Anonimización de tal forma que el Titular no pueda ser identificado o reidentificado (*cf.* definición de 'Anonimización', *infra*).

Los Principios están relacionados entre sí y deberían interpretarse en conjunto, con una perspectiva transversal de género y de derechos humanos que identifique los impactos diferenciados del Tratamiento de Datos y los haga visibles para que tanto los Responsables como los Encargados de los Datos Personales puedan tomar las medidas necesarias para mitigar estas disparidades e impedir que el Tratamiento menoscabe la dignidad y la privacidad de las personas que enfrentan situaciones de especial vulnerabilidad.

[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).

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, reconocidos por los principales sistemas de derechos humanos del mundo.

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) y en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer ("Convención de Belém do Pará") (1994). Asimismo, 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 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 han adoptado algún tipo de legislación con respecto a la protección de la privacidad y los Datos Personales (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, y la protección de la privacidad, la identidad, la dignidad y la reputación.

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 con la tutela de otros derechos fundamentales, tales como la libertad de expresión y el acceso a la información pública o con el interés público.

[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.

El concepto del libre flujo de información

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 de la OEA; 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 (Anexo A). Estos derechos civiles y políticos esenciales se reflejan en las Américas en la constitución y las leyes fundamentales de todos los Estados Miembros (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 la región de las Américas, el acceso a la información pública y de manera especial el acceso a la digitalidad se han caracterizado por la desigualdad y una brecha digital ampliamente documentada, entre otros en virtud de género. 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.

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.

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 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. La frase no abarca la información que no identifique a una persona en particular (o no puede usarse de manera razonable para identificarla).

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 Responsable 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.

A efectos de estos Principios, solo la gente (personas físicas en lo individual o agrupadas en una persona jurídica) 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 derechos e intereses legítimos en materia de privacidad que deberían reconocerse y protegerse efectivamente en la legislación nacional.

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, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal. En ciertas circunstancias podría considerarse que estos datos merecen 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.

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.

Encargado de los Datos

Tal como se usa en estos Principios, el término "encargado de los datos" se refiere a la persona física o jurídica, entidad privada o autoridad pública, ajena a la organización del Responsable de los Datos, que presta sus servicios para llevar a cabo el Tratamiento de Datos Personales.

Responsable de los Datos

Tal como se usan en estos Principios, el término "Responsable de los Datos" se refiere a 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 Tratamiento y la protección de los Datos Personales en cuestión. Tales personas determinan el contenido, las finalidades y el uso de los Datos Personales.

Titular de los Datos

Tal como se utiliza en estos Principio, este término se refiere a la persona cuyos Datos Personales se recopilan, procesan, almacenan, utilizan o difunden.

Tratamiento de Datos

En estos Principios, el término "Tratamiento de Datos" se usa en un sentido amplio y abarca toda operación o conjunto de operaciones realizado con Datos Personales, incluyendo, de manera enunciativa más no limitativa, la recopilación, acceso, organización, adaptación, indexación, aprovechamiento, registro, almacenamiento, alteración, recuperación, divulgación o transferencia.

Principios Actualizados **Anotados**

Principio **uno**

Principio **uno**

Finalidades Legítimas y Lealtad

Los datos personales deberían ser recopilados solamente para finalidades legítimas y por medios leales y legítimo.

Este Principio abarca dos elementos: 1) las "finalidades legítimas" para las cuales se recopilan inicialmente los datos personales y 2) los "medios leales y legítimos" 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 legitimidad y lealtad desde el comienzo, cuando se recopilan inicialmente los Datos. Desde luego, estos Principios se aplican y deberían respetarse en todas las etapas del Tratamiento (a saber, 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 y se respeten si se recalcan y se respetan desde el comienzo.

Finalidades Legítimas

El requisito de legitimidad en las finalidades para las cuales se tratan 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 las finalidades legítimas del Tratamiento de Datos Personales. Como regla general, éstos podrían incluir casos en los que: (a) el Titular de los Datos otorgue su consentimiento expreso para el Tratamiento de sus Datos Personales para una o varias finalidades específicas; (b) el Tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación a petición de éste de medidas precontractuales; (c) el Tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al Responsable de datos; (d) el Tratamiento sea necesario para proteger intereses vitales del Titular o de otra persona; (e) el Tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al Responsable de Datos; (f) el Tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el Responsable de Datos; (g) el Tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente; y (h) el Tratamiento sea necesario para el reconocimiento o defensa de los derechos del Titular ante una autoridad pública.

El requisito de legitimidad abarca el concepto de legalidad y excluye el Tratamiento arbitrario y caprichoso 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 el requisito de legitimidad si el recopilador o Encargado de los Datos informa al Titular 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 las finalidades para las cuales se recopilan los datos, a fin de que la persona pueda entender cómo se recopilarán, usarán o divulgarán los datos.

Medios leales y legítimos

El Principio Uno también requiere que los medios que se empleen para recopilar Datos Personales sean "leales y legítimos". Los Datos Personales se recopilan por medios leales y legítimos cuando la recopilación es compatible tanto con los requisitos legales aplicables como con las expectativas razonables de las personas basadas en su relación con el Responsable 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 telemarketing, 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 sensible.

La "lealtad" 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 sus Datos Personales a los Responsables de los 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 Encargado 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 Responsables 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 "lealtad" separado del tema del engaño, con el fin de evitar Tratamientos de Datos Personales que den lugar a una discriminación injusta o arbitraria contra los titulares.

Principios Actualizados **Anotados**

Principio **dos**

Principio **dos**

Transparencia y Consentimiento

Antes o en el momento en que se recopilen, se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para los cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida 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 previo, libre, inequívoco e informado de la persona a que se refieran.

Este Principio también se centra en la recopilación de Datos Personales como primera etapa de su Tratamiento. 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 tratados, las finalidades para las cuales se traten los Datos Personales, así como los destinatarios o categorías de destinatarios a quienes se divulgarán los Datos Personales y los derechos del Titular de los Datos Personales en relación con los Datos a ser tratados, generalmente a más tardar en el momento en el cual se inicie la recopilación; y (ii) cuando el Tratamiento se base en el consentimiento, se recopilen Datos Personales solo con el consentimiento claro de la persona a la que se refieran.

Transparencia

Antes o al momento de recopilarse los Datos Personales, deberían especificarse claramente: i) la identidad y datos de contacto del Responsable; ii) las finalidades del Tratamiento; iii) el fundamento jurídico de su Tratamiento; iv) los destinatarios o categorías de destinatarios a los cuales los Datos Personales serán comunicados; v) la información a serles transmitida, y vi) la existencia, forma y mecanismos o procedimientos a través de los cuales los Titulares de Datos Personales podrán ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.

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 al tratamiento de sus datos no puede ser válido.

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.

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 las finalidades previstas. Por lo tanto, el consentimiento de la persona debería basarse en suficiente información y debería 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 Tratamiento y toda divulgación que pueda efectuarse. La persona debería ser capaz de efectuar una elección real y 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 Responsable de los 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.

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 Tratamiento legítimos.

El intercambio y la retransmisión de Datos entre los Responsables de los datos plantean algunas cuestiones difíciles. 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 Responsables o Encargados de Datos. Se debería informar a las personas sobre esos intercambios adicionales y ofrecerles oportunidades apropiadas para que den su consentimiento.

Contexto

El requisito del consentimiento debería interpretarse de manera razonable en el entorno tecnológico en rápida evolución en el cual se tratan 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 Tratamiento y la divulgación de Datos satisfagan intereses legítimos. El consentimiento implícito podría ser apropiado cuando los Datos en cuestión no sean Datos Personales Sensibles y cuando se proporcione información razonable sobre las finalidades 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 a partir de interacciones anteriores con Responsables 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 Responsables de los Datos.

Como se ha señalado anteriormente, en unos pocos casos podría autorizarse la recopilación de algunos Datos Personales sin consentimiento cuando el responsable cuente con fundamentos legales alternativos, establecidos en el derecho interno o en el derecho internacional. En esos casos, la parte que recopile y trate los Datos debería demostrar que tiene una necesidad clara de hacerlo para proteger 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.

En algunas situaciones, particularmente en el contexto de la acción humanitaria, obtener el consentimiento puede ser muy difícil y, por ende, puede ser necesario y legítimo recurrir a otro fundamento jurídico, como el interés público o los intereses vitales del Titular de datos. La posibilidad de basarse en motivos de interés público es particularmente relevante para organizaciones humanitarias que, debido a la naturaleza de sus actividades y las situaciones de emergencia en las que generalmente operan, tienen mayores dificultades para obtener consentimiento válido, particularmente el que sea dado de manera informada y libre. Esto puede ser el caso, por ejemplo, cuando el Tratamiento de Datos Personales sea un prerrequisito para recibir asistencia, o cuando se requieran recopilar los Datos de una persona desaparecida. En estos casos, las organizaciones humanitarias deberían fundamentar y motivar claramente su recopilación.

La condición de los "intereses legítimos" no se cumplirá si el Tratamiento 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 Tratamiento de Datos de acuerdo con la condición de los intereses legítimos deberían ser justos y legítimos y ceñirse a todos los principios de la protección de Datos.

Los Datos Personales Sensibles solamente deberían procesarse sin el consentimiento explícito de su Titular 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 las finalidades del Tratamiento 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 Tratamiento 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, salvo que la finalidad del Tratamiento subsecuente de los Datos sea distinta a la originalmente aceptada por el Titular.

El Titular debería tener derecho a retirar su consentimiento de manera expresa en cualquier momento, para lo cual el Responsable deberá establecer mecanismos sencillos, ágiles, eficaces y gratuitos. En general, el retiro del consentimiento no afecta la validez del Tratamiento que se hubiere hecho sobre la base del consentimiento antes de su retiro, siempre y cuando dicho retiro no esté motivado por una intención del Titular de evadir alguna responsabilidad contractual o legal, o incurrir en cualquier otra conducta ilegal o fraudulenta.

Principios Actualizados **Anotados**

Principio **tres**

Principio **tres**

Pertinencia y Necesidad

Los datos personales deberían ser únicamente los que resulten adecuados, pertinentes y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior.

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 y ulteriormente traten los Datos. Las consideraciones contextuales incluyen qué Datos particulares se recopilan y con qué finalidades.

Pertinencia

El requisito de que los Datos sean "pertinentes" significa que deberían guardar una relación razonable con las finalidades para las 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 finalidades con los cuales no guarden ninguna relación.

Necesidad y proporcionalidad

Por lo general, los Encargados de Datos deberían tratar Datos Personales solamente de una forma acorde con las finalidades expresas de su recopilación; por ejemplo, cuando sean necesarios para proporcionar el servicio o el producto solicitado por la persona. Asimismo, los recopiladores y Encargados 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 la finalidad expresa. 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 finalidad legítima y si los beneficios alegados excederán los costos previstos.

En el contexto del Tratamiento 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 Tratamiento 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 del Tratamiento de Datos está evolucionando continuamente desde el punto de vista tecnológico. En consecuencia, debería entenderse que este Principio abarca una medida razonable de flexibilidad y adaptabilidad.

Principios Actualizados **Anotados**

Principio **cuatro**

Principio **cuatro**

Tratamiento y Conservación Limitados

Los datos personales deberían ser tratados y conservados solamente de manera legítima no incompatible con las finalidades para las cuales se recopilaron. Su conservación no debería exceder del tiempo necesario para cumplir dichas finalidades, de conformidad con la legislación nacional correspondiente.

En este Principio se enuncian dos premisas fundamentales con respecto al Tratamiento y la conservación de Datos Personales: 1) los Datos deberían ser tratados y conservados solamente de una manera legítima que no sea incompatible con la finalidad para la cual se hayan recopilado (lo cual se denomina a veces el "principio de finalidad" o de "limitación de la finalidad") y 2) no deberían conservarse más del tiempo necesario para cumplir su finalidad y de conformidad con la legislación nacional correspondiente.

Tratamiento limitado

Con respecto a la primera premisa, los Datos Personales deberían tratarse con finalidades determinadas, específicas, explícitas y legítimas. El Tratamiento y la conservación de Datos Personales deberían ser compatibles con las expectativas razonables de las personas, su relación con el Responsable que recopile los Datos y el aviso o los avisos proporcionados por el Responsable de datos.

No deberían tratarse ni conservarse Datos Personales con finalidades que no sean compatibles con aquellas para las 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 finalidad general en relación con la 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.

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 Tratamiento o "incompatible" de los Datos del Titular y que no estaría permitido salvo que el Titular diera su consentimiento expreso.

El Tratamiento ulterior de Datos Personales con fines archivísticos, investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se consideraría incompatible con las finalidades iniciales. No obstante, dicho tratamiento ulterior seguiría sujeto a este Principio de Tratamiento Limitado y Conservación.

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 Tratamiento más amplio (o "agregado") de Datos de un gran número de personas por el Responsable de datos; por ejemplo, para la elaboración de inventarios o con fines estadísticos o de contabilidad.

Conservación limitada

Los Datos Personales deberían conservarse de forma que se permita la identificación de sus Titulares únicamente durante el tiempo que sea necesario para las finalidades del Tratamiento de los Datos Personales. La realidad

de la tecnología moderna exige una limitación general para la conservación de los datos. Como el costo del almacenamiento de datos ha disminuido considerablemente, suele ser menos costoso para los Responsables de Datos almacenarlos indefinidamente en vez de examinarlos y borrar los que no sean necesarios. No obstante, la conservación innecesaria y excesiva de Datos Personales tiene evidentemente implicaciones para la privacidad. Como regla general, por lo tanto, los Responsables deberían disponer de los Datos de manera segura y definitiva a través, por ejemplo, de eliminarlos sus archivos, registros, bases de datos, expedientes o sistemas de información, 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.

Los Datos Personales podrían conservarse durante períodos más largos siempre que se traten exclusivamente con fines archivísticos, de investigación científica e histórica o fines estadísticos, todos ellos en fin del interés público y sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas para proteger los derechos y libertades del Titular.

Asimismo, las personas deberían poder optar por dar su consentimiento, ya sea de manera expresa o implícita, para que traten y conserven sus Datos Personales con finalidades adicionales. La legislación interna pertinente podría establecer requisitos legales específicos para la conservación de Datos. Igualmente, un Responsable de Datos podría tener razones legales legítimas para conservarlos durante un período mayor al requerido; esto puede darse, por ejemplo, para cumplir otras obligaciones legales –de derecho nacional o internacional– o contractuales, o bien para proteger los derechos, la seguridad o los bienes de la persona, del Encargado de los Datos o de un tercero. Por ejemplo, los empleadores podrían conservar expedientes de exempleados o los médicos podrían conservar expedientes de expacientes a fin de protegerse de ciertos tipos de acción judicial, como juicios por negligencia médica, despido ilegal, etc.

Principios Actualizados **Anotados**

Principio **cinco**

Principio **cinco**

Confidencialidad

Los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley.

Este Principio deriva del deber básico del Responsable de Datos de mantener la "confidencialidad" de los Datos Personales en un entorno seguro y controlado.

Este deber requeriría que el Responsable 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 consentimiento de la persona afectada, en consonancia con las expectativas razonables de la persona afectada o por mandato de la ley. En este último caso, la ley podría autorizar dicha divulgación para garantizar el cumplimiento de obligaciones contractuales y legales, la protección de intereses públicos y privados legítimos. Esta responsabilidad emana de la naturaleza misma de los Datos Personales.

Este deber está directamente correlacionado con aquel contenido en el Principio Seis de proteger 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 esta "autodeterminación en lo que respecta a la información" es el establecimiento y mantenimiento de la confianza entre el Titular de los Datos y el Responsable de datos, especialmente con respecto a la divulgación de Datos Personales a terceros.

La divulgación de Datos Personales a las autoridades encargadas de hacer cumplir la ley y a otras agencias gubernamentales, cuando sea realizada de conformidad con la legislación nacional, no contravendría este Principio. La legislación nacional debería autorizarlo 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 al Capítulo IV de la Ley Modelo Interamericana sobre Acceso a la Información Pública 2.0, aprobada por la Asamblea General de la OEA en 2020, conforme a la cual los sujetos obligados deben proteger la información confidencial de las personas y en particular, los Datos Personales cuya divulgación requiera autorización de sus Titulares.

Principios Actualizados **Anotados**

Principio **seis**

Principio **seis**

Seguridad de los Datos

La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, la pérdida, destrucción, daños o divulgación, aún cuando éstos ocurran de manera accidental. Dichas salvaguardias deberían ser objeto de auditoría y actualización permanente.

De acuerdo con este Principio, los Responsables de los Datos deberían establecer y mantener las medidas de carácter administrativo y técnico 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 tratados ni divulgados excepto con el consentimiento de la persona o de otra autoridad legítima, ni sean accidentalmente perdidos, destruidos o dañados[1].

En términos generales, las medidas adoptadas para proteger los Datos Personales deberían ser elegidas tomando en cuenta, entre otros factores: i) la posible afectación a los derechos de los Titulares, en particular, el posible valor de los datos para una tercera persona no autorizada para su tratamiento; ii) los costos de su implementación; iii) las finalidades del tratamiento, y iv) la naturaleza de los Datos Personales tratados, en especial los Datos Sensibles.

[1] Véase, en este sentido, el artículo 15 ("Medidas mínimas de seguridad para documentación con datos personales") de la Ley Modelo Interamericana sobre Gestión Documental (http://www.oas.org/es/sla/ddi/docs/acceso_informacion_propuesta_ley_modelo_2.0.pdf).

La índole de las salvaguardias implementadas podría variar según la sensibilidad de los datos en cuestión. Evidentemente, los Datos Sensibles requieren un nivel más alto de protección, a la luz de riesgos como por ejemplo, la 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 vulneración de la intimidad sexual, o actos de violencia de género digital.

No obstante, en el contexto moderno, es técnicamente imposible garantizar la privacidad absoluta y la protección completa de los Datos Personales, puesto que 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 una valoración razonada e informada y no necesariamente se vulneraría cada vez que un Responsable de Datos experimente un acceso no autorizado, pérdida, destrucción, daño, uso, modificación o divulgación de los Datos Personales en su poder, siempre y cuando las medidas y salvaguardias implementadas hayan sido "razonables y adecuadas".

La determinación sobre la razonabilidad y adecuación de las salvaguardias debería basarse en métodos y técnicas de seguridad de los Datos consistentes con las buenas prácticas comúnmente aceptadas, al igual que en factores como: i) la evolución constante de las amenazas a la privacidad, especialmente las cibernéticas; ii) los métodos y técnicas más avanzados que estén en uso en el ámbito de la seguridad de los Datos, iii) el contexto de la situación general, y iv) la proporcionalidad y necesidad de las medidas tomadas.

Así pues, una práctica que hace solo unos meses era permisible podría considerarse en la actualidad como 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. El reto consiste en proporcionar orientación válida a los Responsables de los 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 ese sentido, las medidas tomadas deberían revisarse, evaluarse, auditarse, actualizarse y mejorarse periódicamente.

La protección de la privacidad implica también permitir que las personas controlen su experiencia "en línea". Además de tomar medidas de seguridad eficaces, los Responsables 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.

Vulneración de la seguridad de los Datos Personales

La incidencia creciente de intrusiones externas ("vulneración de la seguridad de los Datos Personales"), que consisten en el acceso no autorizado a Datos protegidos, suscita preocupaciones relacionadas con la privacidad y tiene incluso implicaciones en el ámbito penal. En estos casos, los Responsables de los Datos deberían notificar a las personas cuyos Datos hayan sido (o puedan haber sido) comprometidos, así como a las autoridades penales o civiles relevantes. muchos países, entre los cuales se cuentan Estados Miembros de la OEA, la notificación es obligatoria por ley en esos casos.

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 vulneración. Las notificaciones también podrían ofrecer incentivos a los Responsables de los Datos para asumir la responsabilidad, examinar las políticas en materia de conservación y retención de Datos y mejorar sus medidas de seguridad.

Al mismo tiempo, las leyes sobre notificación de vulneraciones de la seguridad de los Datos podrían imponer a los Responsables de los Datos la obligación de cooperar con las autoridades encargadas de hacer cumplir la ley 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 autoridades encargadas de hacer cumplir la ley 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 Responsables de los Datos con respecto a la notificación y la confidencialidad.

En los casos en que se impongan sanciones a los Responsables de los 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 "vulneración de la seguridad de los Datos Personales" (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 Responsable de Datos en caso de una divulgación de ese tipo.

Principios Actualizados **Anotados**

Principio **siete**

Principio **siete**

Exactitud de los Datos

Los datos personales deberían mantenerse exactos, completos, y actualizados hasta donde sea necesario para las finalidades de su tratamiento, de tal manera que no se altere su veracidad.

La exactitud y la precisión revisten una importancia vital para la protección de la privacidad. Los Datos inexactos pueden perjudicar tanto al Encargado de Datos como al Titular, pero en una medida que varía mucho según el contexto.

Cuando se recopilan Datos Personales y se les retiene para seguir usándolos (en vez de hacerlo una sola vez o durante períodos cortos), el Responsable 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 sea necesario para las finalidades para las cuales se hayan recopilado y se traten.

A fin de cumplir sus obligaciones con respecto a la exactitud, los Responsables de los datos deberían dar a las personas una oportunidad razonable para examinar o corregir la información personal que les hayan suministrado, o para solicitar la supresión de dichos datos. Se podría establecer un plazo razonable para la vigencia de este requisito.

Al tomar medidas para determinar la exactitud de los Datos Personales de un Titular ("calidad de los datos"), el Responsable podría considerar la sensibilidad de los Datos Personales que recopile o mantenga y la probabilidad de que éstos 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 Tratamiento limitado y conservación, los Datos Personales que se traten deberían corresponder al mínimo requerido para lograr las finalidades específicas 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 las finalidades 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 Encargados traten y conserven algunos Datos inexactos o fraudulentos.

Principios Actualizados **Anotados**

Principio **ocho**

Principio **ocho**

Acceso, Rectificación, Cancelación, Oposición y Portabilidad

Se debería disponer de métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados, puedan solicitar el acceso, rectificación y cancelación de los mismos, así como el derecho a oponerse a su tratamiento 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 y estar en conformidad con los estándares internacionales aplicables.

Las personas deberían tener derecho a saber si los Responsables 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 Responsable 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. Las personas deben también tener derecho a cancelar sus Datos Personales, a objetar su Tratamiento, y cuando. sea aplicable, a la portabilidad de sus Datos[1].

Sus elementos esenciales son: i) 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

[1] Véase, en este sentido, Artículo16 "Ejercicio de los derechos de acceso, rectificación y cancelación de los datos personales", de la Ley Modelo Interamericana de Gestión Documental.

dichos Datos y por qué; y ii) la capacidad de 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, envío o certificación de los Datos.

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 Tratamiento 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 Responsable acredite tener motivos legítimos para que el Tratamiento prevalezca sobre los intereses, los derechos y las libertades del Titular; 3) cuando el Tratamiento 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.

Los mecanismos previstos en la legislación nacional deberían incluir medios adecuados para que las personas que cuentan con menor acceso a la digitalidad entre ellas las mujeres, las niñas y los grupos en mayor desventaja o con diferentes ejes de exclusión, puedan acceder a los mismos.

En caso de fallecimiento o desaparición del Titular, la legislación nacional de cada Estado podrá reconocer que las personas físicas que sean sus familiares (hasta un determinado grado de consanguinidad) o representantes legales quienes ejerzan los derechos a que se refieren estos Principios respecto de los Datos 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 Responsable, 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.

Los Responsables y Encargados 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.

El derecho de acceso

El derecho de acceso a los Datos Personales mantenidos por un Responsable de los Datos debería ser sencillo de ejercer. Por ejemplo, los mecanismos de acceso deberían formar parte de las actividades regulares del Responsable de los 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 y de una manera razonable. 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.

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 (cf. seccion 'Derecho a la portabilidad de datos', *infra*).

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 Responsable 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 Responsables 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 Responsables de Datos o que impidan de cualquier otra forma que éstos protejan sus derechos, su seguridad o sus bienes, los 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 el derecho internacional o el derecho interno de cada Estado Miembro podrá considerar 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 Responsable 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 Responsable de los 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 Responsable. El Titular de los Datos tampoco tiene necesariamente derecho a compeler al Responsable de los 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 conservados 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. y, en tal caso, 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 Responsables 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 Tratamiento.

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.

Como se mencionó, la legislación nacional de cada Estado debería establecer, en su caso, la existencia del derecho a la cancelación, los requerimientos, plazos, términos y condiciones en que los Titulares podrán ejercer este derecho, así como las causales de improcedencia a su ejercicio.

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 Tratamiento de sus Datos Personales cuando tenga una razón legítima para ello o cuando el Tratamiento 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 Tratamiento con fines de mercadotecnia directa, sus Datos Personales deberían dejar de ser tratados para dichos fines.

El derecho a la portabilidad de los Datos Personales

El alcance del derecho a la portabilidad de Datos Personales es un tema emergente, que continúa siendo discutido al interior de algunos Estados Miembros, en particular respecto a los Datos que abarca y si debe aborDarse de manera general o sectorizada. Un número significativo de Estados Miembros coinciden en que, 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 Responsable en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro Responsable sin impedimento, en caso de que lo requiera.

El Titular podrá solicitar que sus Datos Personales se transfieran directamente de Responsable a Responsable, 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 Tratamiento efectuado por el Responsable 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.

Principios Actualizados **Anotados**

Principio **nueve**

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. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos.

El término "Datos Personales Sensibles" abarca los Datos que se refieren a los aspectos más íntimos de las personas. Estos Datos merecen protección especial porque, si se manejaran o se divulgaran de manera indebida, darían lugar a una intrusión profunda en la dignidad personal, el honor de la persona afectada y sus libertades fundamentales, y podrían desencadenar una discriminación ilícita o arbitraria contra la persona o causar un riesgo de graves perjuicios para la persona.

Los Estados Miembros deberían indicar claramente en su legislación y normativa nacionales las categorías de Datos Personales que se consideren especialmente "sensibles" y que, por consiguiente, requieran una mayor protección. Existe una variedad de aproximaciones a estas categorías entre los Estados Miembros. Según el contexto cultural, social o político, podría incluir, por ejemplo, los Datos relacionados con su salud personal, vida sexual, orientación sexual, 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, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal.

Asimismo, la legislación y la normativa nacionales deberían establecer las garantías apropiadas, que reflejen las circunstancias imperantes en la jurisdicción pertinente a fin de proteger en medida suficiente los intereses de las personas en materia de privacidad y definir el alcance de la prohibición del Tratamiento de Datos Personales Sensibles y las excepciones a la misma. Como regla general, los Datos Personales Sensibles no deberían ser Tratados excepto, por ejemplo, cuando el Titular haya otorgado consentimiento explícito para ello o cuando el Tratamiento sea estrictamente necesario para el ejercicio y cumplimiento de las atribuciones y obligaciones específicas del Responsable de Datos, o para dar cumplimiento a un mandato legal, o razones de seguridad nacional, seguridad pública, orden público, salud pública, o salvaguarda de derechos y libertades de terceros. A manera de ejemplo, la necesidad de protección contra una amenaza transfronteriza grave a la salud pública, como sería una pandemia, podría quedar comprendida en estos supuestos. Al determinar las obligaciones reglamentarias pertinentes, hay que tener en cuenta el contexto en el cual una persona proporciona esos Datos.

Debe recaer en los Responsables 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 quien controla efectivamente los Datos, se podrá proteger mejor a sus Titulares contra daños considerables en una amplia gama de contextos culturales.

Principios Actualizados **Anotados**

Principio **diez**

Principio **diez**

Responsabilidad

Los responsables y encargados del tratamiento de datos deberían adoptar e implementar las medidas técnicas y organizacionales que sean apropiadas y efectivas para asegurar y poder demostrar que el tratamiento se realiza en conformidad con estos Principios. Dichas medidas deberían ser auditadas y actualizadas periódicamente. El responsable o encargado del tratamiento y, en lo aplicable, sus representantes, deberían cooperar, a petición, con las autoridades de protección de datos personales en el ejercicio de sus tareas.

Los sistemas de protección de la privacidad deberían reflejar un equilibrio apropiado entre la reglamentación gubernamental y la implementación ética y efectiva por aquellos que tienen responsabilidad directa por la recopilación, procesamiento, uso, retención y difusión de Datos Personales. 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 Responsables 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 Responsables 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 Responsables de Datos deberían implementar las medidas organizacionales y técnicas necesarias para asegurar y poder demostrar, a petición, que el Tratamiento se realiza de conformidad con estos Principios. Cuando el Tratamiento se realice en nombre de un Responsable, el Responsable debería recurrir solamente a Encargados que garanticen suficientemente la implementación de las medidas técnicas u organizacionales, que permitan que el Tratamiento cumpla con estos Principios y asegure la protección de los derechos del Titular.

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 vulneraciones. La protección de la privacidad depende de una evaluación creíble de los riesgos que el Tratamiento 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 y actualización de las políticas de protección de Datos, así como procedimientos para recibir y responder preguntas y quejas de Titulares. En muchos casos, la designación de un "responsable principal de la información y la privacidad" facilitará la consecución de esta meta.

La adhesión a códigos de conducta o mecanismos de certificación, entre otros, pueden usarse como elementos para demostrar cumplimiento con estos Principios. Por lo tanto, las leyes y normas nacionales en materia de privacidad deberían proporcionar una orientación claramente expresada y bien definida a los Responsables de Datos, incluyendo la exigencia de que rindan cuentas 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 los mecanismos apropiados para responsabilizar a los Responsables de los Datos de las afectaciones 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 Responsables 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.

El concepto de "privacidad por diseño" es una forma de responsabilidad proactiva y se refiere a la etapa previa a la recopilación de los datos, es decir, antes de que inicie su Tratamiento por parte del Responsable o Encargado. En estas primeras etapas es cuando los Responsables o Encargados de los Datos deberían identificar las características y posibles riesgos del Tratamiento al que van a someter los Datos que eventualmente obtengan en función de la tarea que desarrollen, producto que ofrezcan, o servicio que presten.

El diseño del modelo de Tratamiento de Datos asociado con estos productos o servicios debería priorizar la privacidad y la protección de los Datos de los usuarios, de manera consistente con estos Principios y con su legislación nacional, durante todo el tiempo que dure el dicho Tratamiento.

Asimismo, la "privacidad por defecto" está relacionada con el uso proporcional de los Datos personales con la finalidad por la cual se recopilen, conforme a los Principios Tres y Siete. Los Responsables y Encargados de los datos, al igual que los desarrolladores de aplicaciones, sistemas, servicios, plataformas y programas, deberían garantizar que, por el simple hecho de registrarse en su sitio, abrir una cuenta, utilizar su servicio, interactuar con su plataforma o descargar una aplicación, se aplique al usuario la configuración básica de privacidad de manera automática, protegiendo sus Datos Personales conforme requiera la legislación nacional. Las medidas de privacidad por defecto deberían estar completamente implementadas antes de iniciar el Tratamiento de datos personales.

Al implementar tanto la privacidad por diseño como la privacidad por defecto, se debería prestar especial atención a contar con una protección

reforzada de los Datos Personales Sensibles que vayan a ser tratados y, en la medida que lo requiera la legislación nacional, documentar los riesgos identificados y las medidas tomadas para eliminar o mitigar dichos riesgos.

Responsabilidad por compartir Datos con terceros

Los Responsables 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 Responsable de Datos diferente trate Datos Personales en representación de la autoridad (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).

Principios Actualizados **Anotados**

Principio **once**

Principio **once**

Flujo Transfronterizo de Datos y Responsabilidad

Reconociendo su valor para el desarrollo económico y social, los Estados Miembros deberían cooperar entre sí para facilitar el flujo transfronterizo de datos personales a otros Estados cuando éstos confieran un nivel adecuado de protección de los datos de conformidad con estos Principios. Asimismo, los Estados Miembros deberían cooperar en la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o los transmitan a una jurisdicción distinta de la suya, puedan garantizar y 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, por lo cual es deseable que los Estados Miembros de la OEA consideren reconocer estándares interoperables para transferencias transfronterizas de Datos Personales.

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 Tratamiento 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 directriz para que cada Estado Miembro evalúe sus propios mecanismos de protección de la privacidad de cara al flujo transfronterizo de datos personales.

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 mismos Responsables de Datos 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 Responsables y Encargados 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 Tratamiento. Cualesquier restricciones deberían ser no-discriminatorias.

Se alienta a los Estados Miembros a considerar el reconocimiento de estándares interoperables para transferencias transfronterizas a fin de facilitar el flujo 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 dichos Estados, así como incentivar la innovación y reducir las barreras de entrada a la economía global.

Finalmente, se insta a los Estados Miembros a asegurar que la transferencia transfronteriza de Datos Personales entre una organización humanitaria y otra entidad con la finalidad específica de brindar ayuda humanitaria se mantenga libre de restricciones en la medida de lo posible y legalmente permisible. En consecuencia, las legislaciones nacionales deberían tener en cuenta que dichas organizaciones pueden verse en la necesidad de compartir Datos Personales a través de las fronteras para salvaguardar los intereses vitales de los Titulares de los Datos, o para servir al interés público, de conformidad con el mandato de la organización humanitaria.

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 las razones anteriormente expuestas, 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 cooperar

para desarrollar marcos regulatorios y estrategias para 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 Responsables 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 Responsables de Datos

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

Al mismo tiempo, los Responsables 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 Responsables 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 los Datos. 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 medidas 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 un mayor aumento de la capacidad entre las Autoridades Responsables de la Protección de Datos de cada Estado Miembro de la OEA, sobre la base de directrices para asegurar que se cumplan los requisitos básicos de la responsabilización transfronteriza.

Principios Actualizados **Anotados**

Principio **doce**

Principio **doce**

Excepciones

Cualquier excepción a alguno de estos Principios debería estar prevista de manera expresa y específica en la legislación nacional, ser puesta en conocimiento del público y limitarse únicamente a 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 o el interés público.

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 les difunde con rapidez y se les almacena durante mucho tiempo. La finalidad de estos Principios es garantizar 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 tengan que apartarse de estos Principios o establecer restricciones que deberían limitarse a las necesarias, adecuadas y proporcionales en una sociedad democrática para salvaguardar 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 del orden público,

la protección de los derechos y libertades y otros 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 graves a los derechos humanos, las autoridades competentes de los Estados Miembros ya han efectuado arreglos especiales para la cooperación internacional en la detección, investigación, sanción y prevención de delitos penales.

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 respetando los derechos y las libertades fundamentales de los Titulares. Debería haber límites sensatos en la capacidad de las autoridades nacionales para compeler a los Responsables a dar a conocer Datos Personales, manteniendo un equilibrio entre la necesidad de los Datos en circunstancias limitadas y el debido respeto al derecho de los intereses de las personas en materia de privacidad.

Los Estados Miembros deberían abstenerse de solicitar, a través de estas excepciones, Datos personales recopilados por organizaciones humanitarias, cuando el propósito sea utilizarlos con fines no humanitarios, ya que ello podría afectar gravemente a los beneficiarios de los servicios humanitarios en detrimento de su seguridad y de la acción humanitaria en general.

Por medio de leyes o normas públicas, los Estados Miembros deberían indicar claramente esas restricciones y desviaciones respecto de la norma, los casos concretos en que pueda requerirse que los Responsables de Datos divulguen Datos Personales y las razones correspondientes.

Cualquier legislación que tenga como propósito restringir la aplicación de estos Principios debería contener como mínimo, disposiciones relativas a la finalidad del Tratamiento, las categorías de datos personales de que se trate, el alcance de las limitaciones establecidas, las garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas, la determinación del Responsable, los plazos de conservación de los datos personales, los posibles riesgos para los derechos y libertades de los Titulares, y el derecho de los Titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta. Las autoridades nacionales deberían poner tales leyes o normas en conocimiento del público a la brevedad posible.

Principios Actualizados **Anotados**

Principio **trece**

Principio **trece**

Autoridades de Protección de Datos

Los Estados Miembros deberían establecer órganos de supervisión independientes, dotados de recursos suficientes, 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. Los Estados Miembros deberían promover la cooperación entre tales órganos.

La mayoría de los Estados Miembros 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 más, 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 deberá abordar individualmente la naturaleza específica, la estructura, las autoridades y las responsabilidades de estas Autoridades Responsables de la Protección de Datos. La legislación nacional de cada Estado debería dotar a dichas autoridades de la capacidad de cooperar internacionalmente entre sí, así como con las autoridades e instituciones públicas y privadas relevantes –incluyendo las relacionadas al ámbito penal, financiero, del consumidor, entre otras– cuyas labores tengan relación o incidencia con la protección de datos personales.

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 Responsables de Datos y los Encargados 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)[1].

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.

[1] 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).

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques[2].

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 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 Europea 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 debiera considerarse en cambio como parte de un derecho más general a la privacidad[3].

[2] 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.

[3] 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).

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 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

Protección de los datos personales

A continuación, se presenta una selección de los textos de instrumentos internacionales que más probablemente sean útiles para los legisladores y otras autoridades gubernamentales, en orden cronológico por año de adopción.

- Principios rectores de las Naciones Unidas para la reglamentación de los ficheros computadorizados de datos personales, adoptados mediante resolución 45/95 de la Asamblea General de las Naciones Unidas (14 de diciembre de 1990)

- 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 de enmiendas (8 de noviembre de 2001)

- Directiva 2002/58/EC del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas (12 de julio de 2002)

- La Resolución de Madrid: Estándares Internacionales sobre Protección de Datos Personales y Privacidad, adoptada por la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (5 de noviembre de 2009)

- El Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC) (20 de noviembre de 2004), Reglas de Privacidad Transfronteriza de APEC (13 de noviembre 2011), actualización al Marco de Privacidad de APEC aprobada por los ministros de APEC (15 de noviembre de 2016)

- Directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre protección de la privacidad y flujos transfronterizos de datos personales (en vigor desde el 23 de septiembre de 1980, actualizados el 12 de septiembre de 2013)

- Convenio de la Unión Africana sobre Ciber seguridad y Datos Personales (adoptado el 27 de junio de 2014)

- 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

- Reglamento General de Protección de Datos de la Unión Europea ("GDPR" por sus siglas en inglés), en vigor desde el 25 de mayo de 2018

- Protocolo de enmiendas al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal ("Convenio 108 plus", abierto a firma el 10 de octubre de 2018, aún no en vigor)

- Decisión del Secretario-General de la Organización para la Cooperación y Desarrollo Económico (OCDE) sobre la Protección de Individuos en relación con el Tratamiento de sus Datos Personales, en vigor desde el 3 de mayo de 2019

ISBN 978-0-8270-7414-9

OEA

Más derechos para más gente