

CJI/RES. 186 (LXXX-O/12)

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

EL COMITÉ JURÍDICO INTERAMERICANO,

CONSIDERANDO que la resolución AG/RES. 2661 (XLI-O/11) solicitó al Comité Jurídico Interamericano presentar “un documento de principios de privacidad y protección de datos personales en las Américas”;

TOMANDO EN CUENTA la emergencia de una economía de información global basada en el desarrollo de nuevas formas de información digital y de tecnología de la comunicación;

ENFATIZANDO la importancia de la privacidad personal como un derecho humano fundamental;

ENFATIZANDO TAMBIÉN la importancia de la libertad de expresión y de opinión y del libre flujo de información entre fronteras;

TENIENDO EN CUENTA la “Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas” (CJI/doc.402/12), presentada por el relator del tema, el doctor David P. Stewart;

TOMANDO NOTA que cada sistema nacional debería adoptar e implementar una política clara y efectiva de apertura y transparencia respecto a todos los casos, prácticas y políticas relacionados con los datos personales y la información personal,

RESUELVE:

Proponer a la Asamblea General la adopción de los siguientes principios:

Introducción

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

Principio Uno: Propósitos Legítimos y Justos

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

Principio Dos: Claridad y Consentimiento

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

Principio Tres: Pertinencia y Necesidad

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

Principio Cuatro: Uso Limitado y Retención

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

Principio Cinco: Deber de Confidencialidad

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

Principio Seis: Protección y Seguridad

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

Principio Siete: Fidelidad de la Información

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

Principio Ocho: Acceso y Corrección

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

Principio Nueve: Información Sensible

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

Principio Diez: Responsabilidad

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

Principio Once: Flujo Transfronterizo de Información y Responsabilidad

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

Principio Doce: Publicidad de las Excepciones

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

La presente resolución fue aprobada por unanimidad en la sesión celebrada el 9 de marzo de 2012, por los siguientes miembros: doctores Carlos Alberto Mata Prates, David P. Stewart, Fernando Gómez Mont Urueta, Jean-Paul Hubert, Miguel Aníbal Pichardo Olivier, Freddy Castillo Castellanos, Fabián Novak Talavera, José Luis Moreno Guerra y Ana Elizabeth Villalta Vizcarra.