70º PERÍODO ORDINARIO DE SESIONES
26 de febrero al 9 de marzo de 2007
San Salvador, El Salvador

OEA/Ser.Q
CJI/doc.25/00 rev.2
7 febrero 2007
Original: inglés
* Limitado

DERECHO DE LA INFORMACIÓN: ACCESO Y PROTECCIÓN DE LA INFORMACIÓN Y DATOS PERSONALES EN FORMATO ELECTRÓNICO

(Actualización realizada al informe presentado por el doctor Jonathan T. Fried en el 57º período ordinario de sesiones del Comité Jurídico Interamericano, CJI/doc.25/00 rev.1)

INTRODUCCIÓN

1. Antecedentes

La Asamblea General solicitó, durante su vigésimo sexto período ordinario de sesiones realizado en la ciudad de Panamá en junio de 1996, que el Comité Jurídico Interamericano prestase especial atención a temas relacionados al acceso a la información, y la protección de datos personales asentados en el correo y los sistemas computarizados de transmisión electrónica [AG/RES.1395 (XXVI-O/96)].

Entre 1996 y 1998, el Comité Jurídico orientó sus deliberaciones hacia la *Convención para la protección de los individuos respecto al procesamiento automático de los datos personales* del Consejo de Europa, de 1981*,* y a la posibilidad de elaborar un *proyecto de Convención interamericana de auto-determinación relativa a la información.*

El Comité Jurídico Interamericano concluyó un análisis (OEA/Ser.Q CJI/doc.52/98) de la Convención sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal o Convenio de Estrasburgo en relación con un proyecto preliminar de una Convención americana sobre autodeterminación informativa.

Durante la 53ª reunión celebrada en agosto de 1998, el Comité Jurídico solicitó a la Subsecretaría de Asuntos Jurídicos de requerir información de los Estados miembros de la OEA sobre la legislación, reglamentaciones y políticas nacionales existentes, concernientes a:

a) libertad de, o el derecho de una persona a acceder a, la información que se encuentra en la pose o bajo el control de los gobiernos;

b) la protección de datos personales contra el uso no autorizado en la pose o el control de los gobiernos;

c) libertad de, o el derecho de una persona a acceder a, la información que se encuentre en la pose o bajo el control de entidades privadas (por ejemplo, servicios públicos, bancos o agencias de crédito);

d) la protección de los datos personales contra el uso no autorizado, que se encuentren en la pose o bajo el control de entidades privadas;

e) dimensiones transfronterizas o internacionales de lo supramencionado, y

f) cualquier otra legislación nacional, normas regulatorias o políticas que atañen a los datos personales o información en formato de lectura electrónica o por máquinas, que no se encuentra incluido ya en los puntos a) hasta e) arriba.[1]

La Secretaría General solicitó esta información el 8 de diciembre de 1998, a través de la Nota N OEA/2.2/39/98. Seis Estados miembros suministraron los datos en respuesta a la solicitud recibida: Costa Rica, Ecuador, Guatemala, Paraguay, Perú y México.

Con base en la información sometida y una investigación independiente, en agosto de 1999 el entonces relator del Comité Jurídico Interamericano Jonathan T. Fried elaboró un informe titulado *Derecho de información: acceso a y protección de la información y datos personales* (OEA/Ser.Q CJI/doc.45/99), que él mismo presentó al Comité Jurídico Interamericano de la OEA en agosto de 1999. El tema central de dicho informe abarcó las normas regulatorias gubernamentales sobre la información personal, y datos que el gobierno tenía en sus manos.

En su resolución (CJI/RES.9/LV/99), el Comité Jurídico solicitó a la Secretaría General de reiterar su solicitud a los otros Estados miembros de enviar información; lo que se llevó a cabo a través del proceso verbal OEA/2.2/32/99.

Durante el 57º período ordinario de sesiones del Comité Jurídico Interamericano, el Dr. Jonathan Fried, presentó el documento CJ-doc.25-00 rev. 1, Derecho de la información: acceso y protección de la información y datos personales en formato electrónico, el cual se describe con mayor detalle en el siguiente apartado.

El Comité Jurídico Interamericano solicitó a la Subsecretaría de Asuntos Jurídicos, mediante Resolución CJI/RES.13, que remita a conocimiento de los Estados los dos informes preparados por el relator del tema y que reitere a los Estados miembros responder a la brevedad la información que, sobre el tema, les fue requerida.

Durante el 63 período ordinario de sesiones del Comité Jurídico Interamericano (Rio de Janeiro, agosto, 2003), el doctor Alonso Gómez-Robledo sugirió incluir el tema del acceso a la información pública gubernamental en la agenda del Comité. Los miembros del Comité Jurídico acordaron incluir ese tema como tema en seguimiento con el mismo título con el cual aparecía el tema de derecho a la información antiguamente en la agenda, es decir, "Derecho de la Información: Acceso y protección de la información y datos personales".

La Asamblea General durante su 34° período ordinario de sesiones (Quito, junio, 2004), mediante resolución AG/RES.2042 (XXXIV-O/04), tomó nota de la importancia de que este tema haya sido incluido en la agenda del Comité Jurídico Interamericano, y le solicitó que incluya en su próximo informe anual, un informe actualizado sobre la materia.

Durante su 65° período ordinario de sesiones (Rio de Janeiro, agosto, 2004), el Comité Jurídico Interamericano tuvo ante sí el documento CJI/doc.162/04, *Derecho de la información: acceso y protección de la información y datos personales*, presentado por el doctor Alonso Gómez Robledo. El relator del tema subrayó en dicho informe la interdependencia entre la rendición de cuentas y la transparencia en el ejercicio de la democracia.

La Asamblea General durante su 35 período ordinario de sesiones (Fort Lauderdale, junio, 2005), mediante resolución AG/RES.2069 (XXXV-O/05) “Observaciones y recomendaciones al Informe Anual del Comité Jurídico Interamericano”, tomó nota de la importancia del tema y solicitó al Comité que incluya en su próximo informe anual un

[1] OEA/Ser.Q CJI/RES.15/LIII/98.

informe actualizado sobre la protección de los datos personales con base en la legislación comparada.

La Asamblea General de la OEA, durante su 36 período ordinario de sesiones (Santo Domingo, junio, 2006), mediante resoluciones AG/RES.2218 (XXXVI-O/06) y AG/RES.2252 (XXXVI-O/06), solicitó al Comité Jurídico Interamericano que incluya en su próximo informe anual un informe actualizado sobre la protección de los datos personales con base en la legislación comparada. También solicitó al Comité que realice una actualización del estudio "Derecho de la información: acceso y protección de la información y datos personales en formato electrónico" del año 2000 tomando en cuenta los distintos puntos de vista sobre el tema, para lo cual elaborará y distribuirá, con el debido apoyo de la Secretaría, un nuevo cuestionario sobre el tema entre los Estados miembros.

Durante su 69° período ordinario de sesiones (Río de Janiero, Agosto, 2006), y con relación a las resoluciones AG/RES 2218 y AG/RES 2252, se recapitularon las tres tareas específicas encomendadas al Comité: 1) que incluya en su informe anual un informe actualizado sobre el tema de protección de los datos personales con base a legislación comparada; 2) que actualice el estudio específico del Comité Jurídico realizado el año 2000; y 3) que elabore y distribuya un nuevo cuestionario sobre el tema para los Estados miembros de la OEA.

Durante el mismo período el Presidente recordó al Comité Jurídico el informe elaborado por el doctor Jonathan Fried sobre el tema de la protección de datos personales y le solicitó a la Secretaría General la actualización de dicho estudio en materia de legislación comparada a más tardar el día 15 de noviembre de 2006. Se procedió además a la discusión del "Cuestionario para los Estados Miembros de la OEA Respecto a Legislación sobre Acceso a la Información y la Protección de Datos Personales en Vista a la Elaboración de un Instrumento Jurídico", documento CJI/doc.232/06 rev.1, de 17 de agosto de 2006. Después de su consideración, el Comité Jurídico aprobó el documento y solicitó que lo haga llegar a los Estados miembros de la Organización para la elaboración del estudio del Comité Jurídico sobre este tema.

2. Informe del Relator Jonathan Fried

Tal como se señaló anteriormente, sobre la base de una parte de los cuestionarios mencionados en el apartado precedente, el Comité Jurídico Interamericano, a través de su relator, el Dr. Jonathan Fried, presentó en el 57º período ordinario de sesiones del Comité Jurídico Interamericano, el informe CJI/doc.25/00 rev.1, en el se que trata la regulación, mediante instrumentos internacionales así como a nivel de la legislación de algunos países miembros de la OEA, del procesamiento de datos personales en el sector privado. Este informe fue preparado con la asistencia de, y con base en investigaciones profundas realizadas por Thomas Fetz, Asesor Jurídico de la Oficina de Asuntos Jurídicos del Departamento de Relaciones Exteriores y Comercio Internacional de Canadá.

Este informe constituye un valioso aporte no sólo para la comprensión de la verdadera dimensión de este tema, a la luz del impacto que las nuevas tecnologías tienen en ampliar la manipulación y uso de la información de los individuos, sino para ayudar a los Estados a tomar acciones respecto a armonización de leyes, mayor cooperación regional y a encontrar elementos sustanciales para un futuro instrumento regional sobre el tema.

El informe examina la norma reguladora inherente a la protección y acceso a datos personales, guardados en formato electrónico por las organizaciones privadas. Mientras que la protección de los datos en el sector privado puede mejorarse utilizando diversos medios,

inclusive las fuerzas de mercado, tecnología y autorregulación,[2] el enfoque de este informe se orienta a la regulación gubernamental.

Los avances alcanzados por la tecnología de la computación, medicina y biotecnología, han aumentado considerablemente el procesamiento de datos en las diversas esferas de la actividad económica y social. El progreso logrado en la tecnología de la información, ha convertido el procesamiento e intercambio de este tipo de datos a través de las fronteras internacionales en una tarea relativamente fácil. Consecuentemente, el reto consiste en proteger los derechos y libertades fundamentales, especialmente el derecho a la privacidad y el derecho al acceso a la información personal (conocido también como *habeas data*), al mismo tiempo en que se fomenta la libre circulación de la información y comercio electrónico.

3. Actualización

En la Sesión Especial de la Comisión de Asuntos Jurídicos y Políticos conducente a promover, difundir e intercambiar experiencias y conocimientos relativos al acceso a la información pública, celebrada el 28 de abril de 2006 en Washington, D.C., el Relator del Comité Jurídico Interamericano sobre el tema del acceso a la información, Dr. Jaime Aparicio, realizó una presentación en la que se actualizaba el informe del Dr. Fried.

En su presentación el Dr. Aparicio precisó que los mandatos que ha recibido el Comité Jurídico Interamericano, así como el informe presentado por el Comité respecto al tema de acceso a la información, se han limitado sólo a un aspecto de ese vasto tema, que es el del acceso y protección de la información personal de los individuos. Esa información incluye, entre otras, records médicos, records de estudios, historia de crédito, records judiciales antecedentes laborales, records financieros files personales en entidades públicas y privadas, aplicaciones, etc.

Los avances tecnológicos, el internet y otros medios de transmisión de información han puesto en mayor peligro la privacidad de las personas y el derecho a controlar, proteger y evitar la diseminación de su información personal. La protección legal a la privacidad, frente a esta nueva realidad es aun precaria.

Inicialmente las leyes y regulaciones sobre privacidad estaban únicamente referidas al sector público, debido a que eran los Gobiernos quienes mantenían la información personal sobre los individuos. Sin embargo, la utilización de informaciones personales es ahora no sólo un fenómeno entre el Estado y el ciudadano, sino que es cada vez más un tema que involucra al sector privado y a las empresas comerciales que recogen y utilizan la información de los individuos con fines comerciales y por la naturaleza de estas operaciones esa información también pasa las fronteras de los Estados y se convierte en un fenómeno internacional.

La actualizacion de la información presentada por el Dr. Aparicio se llevó a cabo mediante una investigación en coordinación con la Secretaría de la OEA, con la colaboración de la Oficina de Derecho Internacional, lo cual ha permitido recopilar información sobre nuevas leyes o proyectos en la materia, y añadir información sobre algunos países no incluidos en el informe anterior. Sin embargo, se consideró que esta información debería ser nuevamente requerida, a través de la Departamento de Asuntos Jurídicos Internacionales de la OEA a los Estados miembros, para poder contar con información concreta y precisa sobre los avances legales en protección de la información en las Américas.

---

[2] La protección de los datos personales puede lograrse utilizando instrumentos como los contratos de consumidores, políticas de privacidad y códigos de conducta. Por ejemplo, la Cámara de Comercio Internacional ha propuesto y publicado un modelo de contrato para los flujos transfronterizos de datos personales (en-línea: <http://www.iccwbo.org>). Mayores informaciones sobre las políticas modelo, acuerdos y códigos de conducta pueden encontrarse en el sitio Intercambio de Privacidad: <http://www.PrivacyExchange.org>).

En todo caso, y esto no implica que estos sean los únicos países que han realizado avances en la materia, se cuenta con infomación sobre avances en los siguientes países: Argentina, Brasil, Chile, Canadá, México, Estados Unidos, Perú, Uruguay, Colombia, Paraguay, Ecuador, Costa Rica, Panamá y Venezuela.

Teniendo en vista los antecedentes mencionados hasta ahora, el presente informe de actualización pretende integrar el informe del Dr. Fried con la puesta al día presentada por el Dr. Jaime Aparicio y en la que se constatan los cambios producidos en los países señalados, además de proporcionar datos sobre otros países, siempre con la salvedad señalada acerca de la conveniencia de requerir informes actualizados a los países. Esta información puede contribuir a la iniciativa de contar con un marco legal regional que ayude a regular el acceso y la protección de la información.

El presente documento está dividido en tres partes. La primera, discute la regulación del procesamiento de datos en el sector privado utilizando instrumentos internacionales, así como la legislación de algunos estados miembros de la OEA.

En una segunda parte, el informe explica el tratamiento que esos instrumentos internacionales y de algunas legislaciones nacionales al tema de la protección de la privacidad, en el contexto del flujo transfronterizo de los datos personales.

Finalmente, el informe identifica los diversos enfoques existentes para regular la circulación internacional de esa información personal, que abarcan desde la armonización de las leyes de protección de datos personales, al desarrollo de tratados de asistencia mutua.

I. REGULACIÓN DE LA PROTECCIÓN DE DATOS EN EL SECTOR PRIVADO

1. Antecedentes

Inicialmente, las leyes y regulaciones concernientes al acceso y protección de datos personales trataban del sector público. Esto sucedía, comúnmente, porque los gobiernos mantienen mucha información sobre los individuos. Sin embargo, las organizaciones privadas están utilizando cada vez más informaciones sensibles y datos personales, porque los gobiernos fueron descargando varios servicios en el sector privado, a medida que surgían nuevas oportunidades en el campo del comercio electrónico. Las mejorías implantadas en la tecnología, primordialmente en el área de las computadoras y telecomunicaciones, han expandido enormemente las posibilidades de recopilar, almacenar, acceder, y comparar la información personal. Con la expansión de las redes computarizadas, especialmente la Internet, la información puede quedar disponible a miles, si no es que llega a millones de usuarios, simultáneamente, en todo el mundo.[3] Actualmente son más de 150 millones de personas que usan la Internet, estimándose que hasta el año 2003 la cifra llegue a 510 millones. En 1998, la Internet obtuvo entradas de US$301 mil millones, y se espera que esta cifra se multiplique en los próximos años.[4]

Es justamente porque la información personal puede ser de gran utilidad para el mercadeo y áreas de venta, que las organizaciones privadas están buscando constantemente este tipo de información sobre los individuos, ya sea a través de los

---

[3] La Internet se remonta a 1968, cuando se otorgó un contrato para su desarrollo. La Internet física fue construida un año más tarde. La World Wide Web fue introducida en 1992. Michael Power, *Bill C-6: Federal legislation in the age of the Internet*". In: *Manitoba Law Journal* (1999) 26(2): 235.

[4] OEA. Departamento de Derecho Internacional. *Privacy, access to information and the Internet in the European Union, the United States and Latin America: a comparative study*. SG/SLA DDI/doc.01/00. Washington, D.C. : February 2, 2000, p. 3.

métodos tradicionales o a través de la Internet.[5] A menudo, los individuos revelan datos personales voluntariamente en la Internet mientras están visitando sitios comerciales, registrándose en grupos de discusión, participando en competiciones, o expresando sus opiniones. El tipo de información divulgada puede referirse a su nombre, dirección personal y electrónica, números telefónicos, ocupación, ingreso, estado civil, edad, sexo, o detalles sobre su tarjeta de crédito. Además, los usuarios de las tecnologías digitales muchas veces producen "huellas electrónicas", o sea, información digital sobre donde han estado, qué es lo que estaban mirando, los mensajes que han enviado, y los bienes y servicios que han comprado. Por ejemplo, la "navegación" por la Internet siempre deja un cierto "encabezamiento de información" que puede revelar:

a) la dirección del Protocolo Internet (IP) que contiene el nombre del dominio y el nombre y localización de la organización que registró el nombre de dominio;

b) información sobre los usuarios que operan plataformas de sistemas y de hardware;

c) hora y fecha de la visita;

d) el *Uniform Resource Locator* (URL) de la página Web que se ha visualizado anteriormente;

e) la pregunta colocada en una máquina de búsqueda, si corresponde, o

f) la dirección electrónica (e-mail) del usuario, si se encuentra registrada en la pantalla de configuración favorita del *Browser.*

Además, mientras se está *navegando* a través del sitio Web, al salir, un usuario puede dejar "un flujo de datos al pulsar" que suministra información sobre las páginas visitadas, el tiempo utilizado mirando una página y la información enviada y recibida. Esta recopilación de información sobre los usuarios puede tornarse aún más fácil con el uso de los "*cookies*" que no son otra cosa que pequeños paquetes de datos enviados desde el servidor del sitio de la Web al disco rígido del usuario. Estos *cookies* asignan una contraseña única a cada visitante, y el servidor puede accederlos cuando el usuario vuelve a visitar el sitio de la Web. Algunos *cookies* permiten que el usuario acceda rápidamente el sitio de la Web, pero sólo pueden usarse para rastrear los movimientos del usuario en la Web. Aunque este tipo de tecnología tenga sus ventajas, también aumenta el riesgo de la colecta automática, uso y divulgación de los datos, sin el conocimiento o consentimiento de la persona.[6]

Tal cual ocurre en el sector público, los datos personales mantenidos en el sector privado pueden quedar sujetos a una colecta, uso, o divulgación no autorizados, ya sea deliberada o accidentalmente, razón por la cual deben tomarse medidas para minimizar esta actividad. No obstante, la regulación de la protección de y acceso a datos personales debe permanecer sensibilizada a las necesidades de los sujetos a quienes se refieren estos datos, incluyendo entre ellos a los usuarios y consumidores así como también las empresas comerciales y otras organizaciones involucradas. Estas necesidades no son necesariamente contradictorias. Por ejemplo, una de las características esenciales es la confianza que se debe sentir en la protección de la privacidad en línea, para asegurar el crecimiento del comercio electrónico.[7] Los consumidores están preocupados sobre el

---

[5] Según algunas referencias, existen muchas personas que consideran que el tema de la colección de información personal sobre los individuos y sus preferencias para utilizarlos como consumidores objeto, también denominado "*data mining"*, es una total invasión de la privacidad.

[6] Organización de Cooperación y Desarrollo Económico; Dirección de Ciencias, Tecnología e Industria; Comité para las Políticas sobre la Información, Computación y Comunicación; Grupo de Trabajo sobre la Seguridad y Privacidad de la Información; "*Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks*" DSTI/ICCP/REG (98)12/FINAL, (19 mayo 1999) p. 7-8.

[7] El crecimiento del comercio electrónico también trae a colación varios otros temas relativos a la protección del consumidor. La Organización de Cooperación y Desarrollo Económico ha publicado recientemente su "*Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce*"

derecho a la privacidad en un ambiente cada vez más interconectado electrónicamente, y las empresas comerciales desean asegurar su fiabilidad a los consumidores y evitar las interrupciones durante el flujo de datos transfronterizos. En otras palabras, la protección de datos es una cuestión de encontrar el equilibrio perfecto entre los derechos de los individuos a que sus datos personales permanezcan privados, y resguardar el libre flujo de información. Sin embargo, tal como ocurre con otros temas, los estados pueden no concordar donde yace el equilibrio adecuado, o si la protección de datos corresponde a una cuestión de derechos humanos o se inclina más hacia una cuestión económica.

2. Instrumentos internacionales

Se han realizado algunos esfuerzos al nivel internacional para establecer principios comunes sobre la protección de los datos personales en el sector privado. Aunque el efecto directo de los instrumentos internacionales varía, varios han ejercido una influencia muy clara sobre las leyes nacionales y los mecanismos auto-regulatorios relativos a la protección de la privacidad.

a) Instrumentos internacionales de derechos humanos

El derecho a la privacidad se encuentra exaltado en varios instrumentos internacionales de derechos humanos.[8] El Artículo 12 de la *Declaración universal de los derechos humanos*[9] declara como sigue:

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

El Artículo 17 del *Pacto internacional sobre derechos civiles y políticos*[10] utiliza términos casi idénticos:

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio, o su correspondencia, ni de ataques ilegales a su honra y reputación.
2. Toda persona tiene derecho a la protección de la ley contra esas injerencias y esos ataques.

La *Convención americana sobre derechos humanos*[11] se rige por la protección expresa de la "vida privada" en su Artículo 11:

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

[Recomendación del Consejo de la OCDE para la Protección del Consumidor dentro del Contexto del Comercio Electrónico] (19 dic. 1999). En-línea: OCDE: <http://www.oecd.org/dsti/sti/it/>.

8 Vea: Lee A. Bygrave, "*Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*" [Protección de datos de acuerdo con el Derecho a la Privacidad contenido en los Tratados de Derechos Humanos]. In*: International Journal of Law and Information Technology* (1998) 6(3): 247.

9 En-línea: Alto Comisionado de las Nacional Unidas para los Derechos Humanos, Tratados: <http://www.unhchr.ch/udhr/lang/eng.htm>.

10 En-línea: Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Tratados: <http://www.unhchr.ch/html/menu3/b/a_ccpr.htm>.

11 En-línea: *Organization of American States, Treaties and Conventions*: <http://www.oas.org/>.

Artículo 8 de la Convención Europea para la protección de los derechos humanos y libertades fundamentales[12] garantiza el derecho a la privacidad y secreto de su correspondencia:

> 1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> 2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Los tratados y convenciones, que tratan específicamente de la protección de los datos personales, muchas veces mencionan los principios expresados en estos instrumentos de derechos humanos.

b) Lineamientos de la OCDE

El 23 de septiembre de 1980, el Consejo de la Organización de Cooperación y Desarrollo Económico (OCDE) adoptó la *Recomendación concerniente a los Lineamientos que rigen la protección de la privacidad y flujos transnacionales de los datos personalesl*[13] (Lineamientos de la OCDE*)* que suministra los estándares mínimos para la protección de los datos personales. A pesar que los *Lineamientos OCDE* no son obligatorios bajo el derecho internacional, ellos representan, sin embargo, un compromiso político asumido por parte de los Estados miembros. Los Lineamientos OCDE cubren "cualquier información relativa a un individuo identificado o identificable", y se aplican al procesamiento de datos en el sector público y privado.[14]

Los Lineamientos OCDE recomiendan que *"Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines"* y también indican que *"endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data".* Los principios esbozados en los Lineamientos OCDE son los siguientes*:*

Limitación de la colecta

Los datos deben obtenerse por medios legales y justos, y con el conocimiento y consentimiento del sujeto a quien pertenece, cuando fuere necesario.

Calidad de los datos

Los datos personales deben ser importantes para el propósito al que se destinan, así como precisos, completos y actualizados.

Especificación del propósito

Los datos personales deben colectarse y usarse únicamente para fines específicos.

Limitación del uso

---

12 E.T.S. 5, firmado el 11 de abril 1950, entró en vigor el 3 de sept. de 1953; en-línea: Consejo de Europa, Oficina de Tratados, http://conventions.coe.int/treaty/EN/cadreprincipal.htm>.

13 Documento OCDE C(80)58/FINAL (1 octubre 1980); en-línea: OECD: <http://www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm> [de aqui en adelante: Lineamientos de la OCDE].

14 Lineamientos de la OCDE, Parte Uno.

El uso o divulgación de datos personales debe limitarse a un propósito específico, a menos que exista una ley que determine lo contrario o un consentimiento sobre el tema de los datos.

Salvaguardas de seguridad

Deben instalarse salvaguardas de seguridad razonablemente buenas, contra los riesgos inherentes a pérdidas, acceso no autorizado, destrucción, uso, modificación o divulgación de los datos personales.

Transparencia

Las políticas y prácticas referentes a los datos personales deben ser abiertas y transparentes.

Participación individual

Los sujetos de los datos deben tener el derecho de acceder sus datos personales y corregirlos o destruirlos de una manera razonablemente comprensible y costo-tiempo eficiente.

Principio de la responsabilidad

Los gerentes de datos serán considerados responsables por el cumplimiento de las medidas estipuladas en los Lineamientos.[15]

Los Lineamientos de la OCDE recomendaron que los países implanten sus principios a través de: a) la adopción de una legislación apropiada; b) el fomento a la autorregulación; c) el suministro de medios razonables a los individuos para ejercer sus derechos; d) la aplicación de sanciones y remedios adecuados donde falta la conformidad; e) asegurarse que no existe ninguna discriminación injusta contra los sujetos a quienes se refieren los datos.[16] La debilidad fundamental de los Lineamientos de la OCDE, sin embargo, reside en su naturaleza voluntaria.

c) Convención del Consejo de Europa

Contrariamente a los *Lineamientos de la OCDE*, la *Convención para la protección de las personas con respecto al procesamiento automático de los datos personales*[17] del Consejo de Europa es un instrumento legal obligatorio. La *Convención* fue adoptada el 18 de septiembre de 1980, y su suscripción fue abierta el 28 de enero de 1981, entrando en vigor el 1º de octubre de 1985, después de cinco ratificaciones. Cualquier Estado, aún aquellos que no son miembros del Consejo de Europa, pueden adherirse a la Convención. La Convención se aplica al procesamiento automático de datos personales en los sectores público y privado.[18]

La Convención obliga a los Estados a incorporar ciertos principios relativos a la colecta y procesamiento de los datos personales en su ley nacional. Estos principios son similares a aquellos contenidos en los Lineamientos de la OCDE. No obstante, el Artículo 6 de la Convención agrega un principio adicional, disponiendo sobre las salvaguardias relativas a la revelación de información sobre los datos relativos al origen racial, opinión política o religiosa y otras creencias, salud o vida sexual, o condenas criminales. También se requiere de los Estados miembros que establezcan “sanciones y remedios apropiados para la violación de la ley nacional, colocando en vigor los principios básicos”.

---

15 Lineamientos de la OCDE, Parte Dos.

16 Lineamientos de la OCDE, Parte Cuatro.

17 Tratado Europeo, Serie No. 108; Consejo de Europa, Oficina de Tratados: <http://conventions.coe.int/treaty/EN/cadreprincipal.htm> [de ahora en adelante Convención Consejo de Europa].

18 Sin embargo, los Estados están autorizados a limitar el alcance y aplicación de la Convención a través de una declaración dirigida al Secretario General del Consejo de Europa. Convención del Consejo de Europa, artículo 3.

La Convención del Consejo de Europa ha inculcado un significativo impulso a los Estados miembros para aplicar leyes que regulen el flujo de los datos personales. Por sí solo, este no es un instrumento capaz de proteger los datos personales debido al hecho que su interpretación e implementación residen en las autoridades nacionales de los Estados miembros.

En el Artículo 18 de la Convención, el Comité Consultivo ha redactado recientemente un *Protocolo adicional*[19] que trata sobre el establecimiento de autoridades fiscalizadoras y la circulación transfronteriza de los datos. Este proyecto de Protocolo necesitaría que las Partes establezcan autoridades supervisoras independientes, que puedan asegurar el cumplimiento de las leyes nacionales, colocando en vigor los principios estipulados en esta Convención. Estas autoridades de supervisión (comisionados de privacidad o protección de datos u oficiales de protección de datos) escucharían las quejas existentes sobre la violación de las leyes de la privacidad y estarían empoderados para investigar e intervenir, así como para dedicarse a los procedimientos legales cuando las disposiciones sobre la privacidad que constan en las leyes domésticas ha sido violada".[20]

El Consejo de Europa también estimula la autorregulación a través de códigos de conducta con respecto al procesamiento de los datos personales. Por ejemplo, El Comité de Ministros recomendó a los Estados miembros proceder a la divulgación de los *Lineamientos para la protección de los individuos respecto a la colecta y procesamiento de datos personales en la autopista de la información*, dirigidas directamente a los proveedores y usuarios de los servicios de la Internet.[21]

d) Lineamientos de las Naciones Unidas

La Asamblea General de las Naciones Unidas adoptó los *Lineamientos para la regulación de archivos con datos personales computarizados* (Lineamientos de la ONU), emitidos por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos[22] de concordancia con el Artículo 10 de la Carta de las Naciones Unidas de 1990.[23] Los Lineamientos de la ONU, que no son obligatorios, ofrecen los estándares mínimos que los Estados deben adoptar al regular la protección de la privacidad de los archivos computarizados, tanto públicos como privados.[24]

Los principios incluidos en los Lineamientos de las ONU son la legalidad y equidad, precisión, especificación de propósitos, acceso, la no discriminación, empoderamiento para hacer excepciones (seguridad nacional, orden público, salud pública y moralidad, y los derechos de las libertades de los demás), seguridad así como supervisión y sanciones. Estos principios son similares a aquellos que constan en los Lineamientos de la OCDE. Protección adicional, así como supervisión y sanciones. Se ofrece una protección adicional a través de la prohibición de realizar la recopilación de "*data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life,*

---

19 Comité Consultivo de la Convención para la protección de las personas con respecto al tratamiento automático de los datos personales. "*Proyecto de Protocolo Adicional a la convención sobre la protección de las personas con respecto al tratamiento de los datos personales* (ETS No 108) *relativo a las autoridades supervisoras y flujo transfronterizo de los datos*", Strasbourg, 8 junio 2000; web sitio del Consejo de Europa, Protección de Datos Personales. : <http://www.coe.fr/dataprotection/Treaties/projet%20de%20protocole%20E.htm> [de aquí en adelante Proyecto de Convención].

20 Proyecto de Protocolo, Artículo 1.

21 Recomendación No.R (99) 5 del Comité de Ministros de los Estados Miembros para la Protección de la Privacidad en la Internet: Lineamientos para la protección de los individuos con respecto a la colección y procesamiento de los datos personales sobre la autopista de la información (adoptado por el Comité de Ministros el 23 de febrero de 1999 durante la 660ª. Reunión de los Ministros Adjuntos) en el sitio de la Web del Consejo de Europa, Protección de los Datos Personales : <http://www.coe.fr/dataprotection/rec/elignes.htm>.

22 Alto Comisionado de las Naciones Unidas sobre Derechos Humanos: <http://www.unhchr.ch/html/menu3/b/71.htm>.

23 Resolución 45/95, 14 diciembre 1990, en el sitio en la web de las Naciones Unidas, Centro de Documentación: <http://www.un.org/gopher-data/ga/recs/45/95>.

24 Los Lineamientos de la ONU se aplican también a archivos de datos personales en poder de organizaciones gubernamentales internacionales.

political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union". [25]

Los *Lineamientos* de la ONU urgen a los países a designar autoridades independientes, imparciales, y técnicamente competentes para hacerse responsables por la supervisión de los principios estipulados en los *Lineamientos*. Las sanciones aplicables por la violación de los principios deben incluir sanciones criminales apropiadas, u otras sanciones conjuntamente con los remedios individuales.[26]

e) Directiva de la Unión Europea sobre la privacidad

La *Directiva* 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre 1995 *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*[27] (La Directiva de la UE) fue firmada en 1995, para ser implementada por los Estados miembros hasta el 24 de octubre de 1998. Su texto urgía a los Estados miembros a contar con leyes que estableciesen un mínimo nivel de protección sobre el tratamiento de datos personales por cualesquier medios. Los Estados son libres de promulgar leyes con estándares mucho más rigurosos que los determinados por la UE. La Directiva de la UE reconoce que los "datos personales deben circular libremente de un Estado miembros a otro, pero también expresa que los derechos fundamentales de los individuos deben salvaguardarse." La Directiva de la UE se aplica al tratamiento de datos personales por cualquier persona cuyas actividades están regidas por el Derecho Comunitario, en los sectores públicos y privados, pero no abarca las operaciones de procesamiento concernientes a la seguridad pública, defensa, seguridad del Estado, y las actividades que el Estado desempeña en las áreas del derecho criminal. Tampoco se aplica a las actividades de procesamiento de datos de personas naturales durante el curso de su actividad hogareña, puramente personal.[28]

Los principios de protección a la privacidad establecidos en la Directiva de la UE tienen mayor alcance y están más detallados que aquellos inherentes a los *Lineamientos* de la OCDE. Los datos sólo pueden procesarse si el "interesado" ha otorgado un "consentimiento inequívoco".[29] Dicho consentimiento puede ser explícito con respecto a los "datos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, y el tratamiento de los datos relativos a la salud o a la sexualidad."[30] Aún en los casos en que se ha obtenido consentimiento para procesar la información, el interesado debe "ser informado antes de que los datos personales se comuniquen por primera vez a terceros o se usen en su nombre a efectos de prospección de mercadeo, y a que se la ofrezca expresamente el derecho a oponerse, sin gastos, a dicha comunicación o uso."[31]

El procesamiento no consentido sólo puede continuar, generalmente, si existe una de las cinco excepciones. El procesamiento es 1) "necesario para el desempeño de un contrato del cual el interesado es parte"; 2) "necesario para cumplir una obligación legal"; 3) "necesario para proteger los intereses esenciales del interesado"; 4) "en el interés público"; o 5) "el procesamiento se hace necesario para que los intereses legítimos que persigue el *controller* o una tercera parte u otras partes a quienes se están divulgando los datos,

---

25 Lineamientos de la ONU, Artículo 5.

26 Lineamientos de la ONU, Artículo 8.

27 Directiva 95/46/EC, 24 octubre 1995, Boletín Oficial de las Comunidades Europeas , L 281 (23 Noviembre 1995), at 31. El texto de la Directiva de la Unión Europea sobre Privacidad puede encontrarse en el sitio: : Eur-Lex: <http://europa.UE.int/eur-lex/en/lif/dat/1995/en_395L0046.html> [de ahora en adelante Directiva de la UE].

28 Directiva de la UE, Artículo 13.

29 Directiva de la UE, Artículo 7.

30 Directiva de la UE, Artículo 8.

31 Directiva UE, Artículo 14. Las ventas por mercadeo directo en Europa ascendieron a 125 mil millones de dólares en 1997, comparado con los 1.2 billones de dólares en los Estados Unidos. Gregory Shaffer, "*Globalization and Social Protection: The Impact of UE and International Rules in the Ratcheting Up of U.S. Privacy Standards*," (2000) 25 (1). In: *Yale Journal of International Law, p.* 1-18.

excepto cuando dichos intereses están precedidos por los intereses de los derechos y libertades fundamentales del interesado que exige protección."[32]

El interesado debe ser informado sobre la identidad de la parte que controla (la persona que determina el propósito y la forma en que se procesarán los datos); el propósito que se espera alcanzar con el procesamiento de datos, y de cualquier otra información importante para "garantizar un tratamiento justo". Los sujetos de los datos también tienen el derecho a acceder y a corregir o eliminar sus datos personales. Los sujetos de los datos pueden monitorear y oponerse al uso de la información personal durante y después del procesamiento. Ellos pueden rastrear qué terceras partes tienen en sus manos su información personal, verificar cómo la están utilizando, y bloquear usos que no han sido autorizados.[33] Además, ellos también tienen el derecho de impugnar ("de no estar sujetos a") cualquier decisión que los afecte significativamente, tal como una que está fundada en el procesamiento automatizado de datos que se pretende utilizar para evaluar aspectos personales, tales como su desempeño en el trabajo, potencial crediticio, credibilidad, conducta, etc."[34]

Los Estados miembros de la UE son responsables tanto por la implementación como por la ejecución de la Directiva de la UE. Los Estados deben garantizar a los sujetos el derecho a un remedio judicial, y los sujetos cuyos datos han sido utilizados erróneamente deben tener derecho a una indemnización por daños y perjuicios.[35] La implementación de los principios de la Directiva de la UE sobre la protección de la privacidad debe ser reforzada por la autoridad de control. Estas autoridades deben "actuar con total independencia" y estar conferidas de "empoderamiento investigativo" que les permita acceder los datos y colectar la información. Además, ellos deben tener un "efectivo empoderamiento para la intervención" tales como la habilidad de emitir opiniones, tornar público el tema, o determinar el bloqueo o destrucción de los datos. Las autoridades supervisoras o de control también deben tener el empoderamiento para ejecutar los procedimientos legales o traer el tema a la atención de las autoridades judiciales.[36]

f) Acuerdo general sobre el comercio en servicios

Tomando en cuenta el impacto que las normas comerciales ejercen sobre muchos aspectos de la actividad económica y social, debemos mencionar dentro de este contexto el Acuerdo General sobre el Comercio en Servicios [G*eneral Agreement on Trade in Services (GATS)]*[37], que forma parte del marco de los tratados de la Organización Mundial del Comercio (OMS). El Artículo XIV del GATS dispone:

A reserva de que las medidas enumeradas a continuación no se apliquen en forma que constituya un medio de discriminación arbitrario o injustificable entre países en que prevalezcan condiciones similares, o una restricción encubierta del comercio de servicios, ninguna disposición del presente Acuerdo se interpretará en el sentido de impedir que un Miembro adopte o aplique medidas:

(c) (ii) la protección de la privacidad de los particulares en relación con el tratamiento y la difusión de datos personales y la protección del carácter confidencial de los registros y cuentas individuales.[38]

---

32 Directiva de la UE, Artículo 7.
33 Directiva de la UE, Articulos 10, 11 & 12.
34 Directiva de la UE, Artículo 15.
35 Directiva de la UE, Artículos 22-24.
36 Directiva de la UE, Artículo 28.
37 Sitio en la Web - Organización Mundial del Comercio, Textos Legales: <http://www.wto.org/english/docs_e/legal_e/final_e.htm> [de aqui en adelante GATS].
38 GATS, article XIV c(ii).

Consecuentemente, mientras el GATS prohibe la discriminación y las barreras comerciales encubiertas, continúa existiendo bastante espacio para que las autoridades nacionales regulen el flujo transfronterizo de los datos, con el propósito de proteger la privacidad.

3. Legislación nacional

Al nivel nacional, la protección de los datos en las organizaciones que operan en el sector privado ha adoptado la forma de protecciones constitucionales, leyes amplias, leyes sectoriales, autorregulación o la combinación de cualquiera de ellas. Las leyes amplias o globales tienen a aplicar los principios generales de la protección de la privacidad a una amplia gama de sectores, tanto público como privado. Las leyes sectoriales conciernen únicamente a sectores específicos, tales como las comunicaciones, o con datos específicos tales como la información médica. Las leyes de la mayoría de los países incluyen datos generales de los principios de la protección de los datos, disposiciones para las autoridades fiscalizadoras, comúnmente conocidas como comisionados de la privacidad u oficiales para la protección de los datos, y alguna referencia a la autorregulación de la industria. El papel y los poderes asignados a las autoridades fiscalizadoras generalmente se refieren a la educación pública, la investigación de las quejas, y su ejecución. La autorregulación depende de las fuerzas de mercado y de las iniciativas lideradas por la industria para ofrecer soluciones novedosas. Las normas son desarrolladas y aplicadas por aquellos a quienes se aplican. En algunos casos, sin embargo, las entidades independientes o públicas están involucradas en el desarrollo, implementación y ejecución de los lineamientos de los códigos industriales.

En América Latina, la protección de los datos se encuentra íntimamente vinculada al concepto de *habeas data,* que garantiza a todos los individuos el derecho a acceder su información personal. Este concepto se basa en el reconocimiento de que un individuo debe tener control sobre los datos que obtienen sobre su persona. El principio surgió recientemente en respuesta al impacto negativo que emanó del uso de las computadoras sobre los derechos a la privacidad. La Constitución Brasileña de 1988 fue la primera a utilizar la expresión *habeas data*. De ahí en adelante, el derecho de los individuos a acceder su información personal fue incluido en las constituciones nacionales de varios Estados latinoamericanos, entre los cuales están Argentina, Colombia, Paraguay, Perú y Venezuela.[39]

a) Argentina

1) Constitución Argentina

La Constitución Argentina de 1994 contiene disposiciones sobre la protección de la privacidad. El Artículo 18 declara:

El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación.

El Artículo 43 de la Constitución que rige sobre el derecho de *habeas data*, dice:

1. Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por la Constitución, un tratado o una ley.

[39] OEA. *Op. cit*., p 26.

En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.

3. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos.

2) Legislación

En 1996, el Senado y la Cámara de Diputados aprobaron una leydestinada a regir las disposiciones contenidas en el Artículo 43 de la Constitución de 1994.[40] Esta ley fue vetadao por el Presidente Menem después de las intervenciones realizadas por la Asociación de la Banca, que consideró que las disposiciones sobre la divulgación de la privacidad eran demasiado rigurosas, y que tendrían el efecto de minar las operaciones realizadas por VERAZ – una organización de investigación crediticia.

Posteriormente se introdujo la regulación del Habeas Data, mediante la Ley NE 25.326 del 4 de octubre de 2000. Dicha ley estableció los principios generales para la protección de los datos personales, los derechos de los titulares de los datos, reguló lo atinente a los usuarios y responsables de archivos, registros y bancos de datos. La ley cuenta igualmente con un capítulo de control y sanciones e instituye la acción de protección de datos personales.

Como la propia ley lo indica en su articulo 1, su objeto es la “protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados, destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional”. Sus disposiciones son aplicables en cuanto resulte pertinente a los datos relativos a personas de existencia ideal.

La ley diferencia los datos personales de los datos sensibles, estableciendo que la formación de archivos de datos es lícita siempre y cuando se respete lo establecido en la ley. Además, se requiere el consentimiento del titular salvo en los casos de las excepciones establecidas en la propia ley. En cambio, se prohíbe la recolección y tratamiento de datos de carácter sensible salvo por motivos de interés general autorizados en el mismo cuerpo legal. La ley declara expresamente que la Iglesia Catolica, otras asociaciones religiosas, organizaciones politicas y sindicales pueden llevar registro de sus miembros.

La Ley prohíbe la transferencia internacional de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados salvo en los siguientes casos:

-colaboración judicial internacional;
-intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica;
-transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;
-cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

[40] Ley No. 24.745 (23 Dic. 1996).

-cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Entre la normativa que regula el habeas data tambien caben citar los siguientes decretos: Decreto 995/2000, sobre "Habeas Data", publicado en el Boletín Oficial del 2/11/2000, num 29517; y el Decreto 1558/2001, sobre "Protección de datos Personales", publicado en el Boletín Oficial del 3/12/2001.

3) Código Penal

Los Artículos 153-157 del Código Penal prohíben la publicación de comunicaciones privadas. En abril de 1999, la corte consideró que dichas disposiciones también se aplican al correo electrónico. Además, el Código Civil también prohibe la intromisión arbitraria *en la vida ajena publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad"*[41].

b) Brasil

1) La Constitución brasileña

Brasil no tiene una ley específicamente orientada a la protección de los individuos de la colección, uso y divulgación no autorizadas de sus datos personales que se encuentren en formato electrónico en las manos de organizaciones privadas.[42] Sin embargo, es importante notar que la Constitución de 1988, cuyo Artículo 5 garantiza la inviolabilidad de los derechos a la vida, libertad, equidad, seguridad y propiedad, estipulando también que los juicios por *habeas data* son gratuitos. Existen otras leyes que se refieren indirectamente a la protección de la privacidad en el sector privado.

2) Ley No. 9.507

La Ley No. 9.507, de noviembre de 1997, regula sobre el acceso a la información y codifica los procedimientos del *habeas data.* En su texto, la ley considera que "todos los registros o bancos de datos conteniendo información que es transmitida o puede llegar a ser transmitida a terceras partes o cuya intención no es la de ser usada por un organismo privado o una entidad productora o depositaria de información."

3) Ley No. 8.078

El enfoque de la Ley No. 8.078, de septiembre de 1990 (*Código para la Protección y Defensa del Consumidor*), trata sobre la protección del consumidor, vinculado a los derechos del consumidor, relaciones del consumidor, calidad de los productos y servicios, y las responsabilidades de los proveedores. En su Artículo 44, la ley declara que el consumidor tendrá derecho a acceder a los datos personales relativos a su persona y las respectivas fuentes de información. También permite al consumidor revisar y exigir la inmediata corrección de los datos que sean erróneos.

4) Legislación propuesta

---

41 Art. 1071bis, Cod. Civ.; Vea: David Banisar y Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments* (1999) 18 (1). In: John *Marshall Journal of Computer & Information Law* 1, p. 15-17.

42 La información sobre la legislación que rige el procesamiento electrónico de datos personales en el Brasil, ha sido suministrada por Luiz Miguel da Rocha de la Embajada de Canadá en Brasilia, el 27 de julio de 2000.

En 1996 el Senado de Brasil introdujo el Proyecto de Ley No. 61 que hubiera regido la creación y uso de registro y bancos de datos personales, tanto públicos como privados.[43] El Proyecto de Ley no ha sido promulgado aún y fue archivado en enero 1999, al terminar el período del Congreso 1994-1998. No obstante lo antedicho, existe otro Proyecto de Ley sobre privacidad en el Senado (No. 268 de 1999), que ya ha sido aprobado por el Comité Constitucional y de Justicia del Senado, que reemplazará a la Ley No. 9.507. La nueva ley, si llega a aprobarse, regirá la estructuración y uso de los bancos de datos y codificará los procedimientos de *habeas data.* Con respecto al objetivo de esta ley, datos personales sobre opiniones raciales, políticas y religiosas, convicciones e ideologías, salud mental y física, sexualidad, prontuario policial, temas familiares, y la profesión, se consideran como datos personales que no pueden divulgarse o utilizarse para cualquier otro propósito que aquel que motivó la creación del banco de datos, excepto a través de una orden judicial, o la autorización de la persona en cuestión. El proyecto especifica que los datos personales disponen sobre datos referentes tanto a la persona física como jurídica.

El proyecto de Ley sobre Privacidad mencionado en el párrafo anterior (268 de 1999) continúa en trámite en el Senado, por lo cual sigue vigente en cuanto al habeas data la ley 9.507.

c) Canadá

Aún considerando que la Constitución de Canadá, inclusive la Carta de los Derechos y Libertades, no reconoce explícitamente el derecho a la privacidad, la Corte Suprema ha interpretado que la Sección 8 de la Carta (que trata sobre la búsqueda y aprensión) garantiza el derecho a una expectativa razonable de privacidad.[44] Canadá cuenta con bastantes leyes bien claras que gobiernan el acceso a y el procesamiento de datos personales. La Ley de Privacidad - *Privacy act*[45] así como la Ley sobre el Acceso a la Información (*Access to information act)*[46] se aplican al sector institucional público federal. Además, la *Ley sobre información personal y documentos electrónicos* [*Personal information and electronic documents]* ha sido aprobada recientemente para regular la protección de los datos en el sector privado. La mayoría de las provincias tienen amplias leyes que cubren el procesamiento de datos en el sector público, pero la Ley de Quebec *respetando la protección de la información personal en el sector privado [Act respecting the protection of personal information in the private sector*] es la única ley global que se aplica al sector privado.

1) Ley sobre información personal y documentos electrónicos

La *Ley sobre información personal y documentos electrónicos*[47] recibió el consentimiento real el 13 de abril de 2000, y entrará en vigor en Canadá el 1º de enero de 2000.[48] El propósito de la Ley es establecer "normas que gobiernen la colecta, uso y divulgación de información personal de tal manera que reconozca el derecho a la privacidad de los individuos respecto a su información personal, y la necesidad de colectar, usar y divulgar información personal para propósitos que cualquier persona razonable consideraría apropiados bajo dichas circunstancias."[49] Al mismo tiempo que protege la privacidad de la información personal, la Ley ha sido creada para dar apoyo y promover el comercio electrónico. Esta nueva ley debería ayudar a Canadá a cumplir los estándares de la protección de datos establecida en la Directiva sobre Privacidad de la Unión Europea.

---

43 Privacy Exchange, Biblioteca Legal, Legislación Nacional/Pendiente, Brasil , Proyecto de Ley del Senado No. 61, 1996": <http://www.privacyexchange.org/>.

44 *Hunter* v. *Southham* [1984] S.C.R. 159, 160.

45 Department of Justice, "Consolidated Statutes" <http://canada.justice.gc.ca/FTP/EN/Laws/Title/P/index.html>.

46 *Department of Justice, "Consolidated Statutes",* <http://canada.justice.gc.ca/FTP/EN/Laws/Title/A/index.html>.

47 S.C. 2000, c-5; Canada Gazette, 23(1), <http://canada.gc.ca/gazette/hompar3-2_e.html> [hereinafter LIPDE].

48 The federal Act provides for several phase-in periods to allow the provinces to adapt to the new legislation. If a province enacts a law that is substantially similar to the federal Act, the organizations or activities covered by the provincial law will be exempted from the federal law.

49 LIPDE, Artículo 3.

La ley entrará en vigor a lo largo de un período de tres años, y eventualmente se aplicará a toda organización privada que recopila, utiliza o divulga información personal en el curso de su actividad comercial, excepto cuando dichas actividades se realicen dentro de la jurisdicción provincial donde una provincia tiene su propia ley substancialmente similar a la ley federal. Hasta la fecha, la provincia de Quebec es la única jurisdicción en América del Norte que tiene este tipo de ley. La Ley no se aplica a individuos respecto a la información personal colectada, utilizada o divulgada únicamente por motivos personales o domésticos. También se hace una excepción para las organizaciones que colectan, usan y divulgan informaciones cuyos propósitos son periodísticos, artísticos o literarios.[50]

La información personal se define como la "información sobre un individuo identificable", inclusive sobre su raza, origen étnico, color, edad, estado civil, religión, educación, antecedentes médicos, criminales, laborales o financieros, dirección y número telefónico, identificadores numéricos como su número de la Previsión Social, huellas digitales, grupo sanguíneo, muestras de tejido y biológicas, y consideraciones y opiniones personales.

La Ley enumera diez principios que rigen la colección, uso y divulgación de información personal:[51] responsabilidad o imputabilidad, identificación de los propósitos para la colección de información personal, obtención de consentimiento, limitando la colección, su uso, divulgación y retención, asegurando la precisión, suministrando seguridad adecuada, colocando fácilmente a disposición las políticas para la administración de la información, brindando acceso a los individuos para acceder a datos sobre sí mismos, y otorgando a los individuos el derecho a objetar y oponerse al cumplimiento que la organización da a estos principios. Informaciones adicionales sobre estos principios constan más abajo.

Responsabilidad - imputabilidad

Las organizaciones son responsables por la información personal que se encuentra bajo su control y deben designar a individuos que controlen el cumplimiento de la Ley. Deben implementarse las políticas y procedimientos, capacitar a los empleados, y la información debe ser suministrada al público para asegurar la protección de la información personal. En los casos en que la información es procesada por una tercera parte, la organización debe usar instrumentos contractuales u otros medios que le permitan suministrar un nivel de protección similar.[52]

Propósitos de identificación

Deben identificarse y documentarse los propósitos para los cuales se ha procesado la información, inclusive los casos donde la colección anterior de información se está utilizando para un propósito nuevo. Es recomendable que los individuos permanezcan siempre informados sobre el propósito antes y durante el período de colección, pero a más tardar antes que la información se utilice.[53]

Consentimiento

Con la excepción de ciertas circunstancias, un individuo debe tener conocimiento y dar su consentimiento si la información personales cuando se va a colectar, usar, o divulgar la información. El consentimiento debe obtenerse después de la colección de los datos pero siempre antes que se la utilice. Para que el consentimiento tenga algún significado, los propósitos del tratamiento de los datos deben ser explicados al sujeto, y las organizaciones deben hacer un esfuerzo razonable para asegurar que los han entendido. La naturaleza y

---

50 LIPDE, Artículo 4.

51 La Ley incorpora como Programa 1, los principios estipulados en el *Código Modelo para la Protección de Información Personal*, de la Asociación Canadiense de Normas.

52 LIPDE, Programa 1, Principio 1.

53 LIPDE, Programa 1, Principio 2.

modalidad del consentimiento puede variar, dependiendo de la sensibilidad de la información, las circunstancias, y las expectativas razonables que tiene el individuo. El consentimiento sólo puede obtenerse para los datos procesados para propósitos legítimos, debidamente especificados. En el caso que una organización quiera utilizar la información para propósitos diferentes a aquellos para los cuales fue colectada, antes de hacerlo debe obtener un nuevo consentimiento. Los individuos tienen el derecho de retirar su consentimiento, sujeto a obligaciones legales o contractuales, después de una notificación previa razonable.

Una organización puede colectar información personal sin el conocimiento o consentimiento de un individuo apenas bajo circunstancias muy limitadas. Esto puede ocurrir cuando la colección claramente representa una ventaja o beneficio para el individuo, o cuando la obtención del consentimiento comprometería la precisión de la información. Además, el conocimiento y consentimiento no se exigen para una investigación legal o asistencia en caso de emergencia que amenace la vida, salud o seguridad del individuo o si la divulgación se exige por ley para propósitos estadísticos o académicos, o para la conservación de registros históricos o de importancia para los archivos.[54]

Limitación de la colecta

La cantidad y tipo de información colectadas debe restringirse a lo que se necesita para propósitos de identificación. Toda información debe ser colectada por métodos justos y legales, que no puedan confundir o engañar a los individuos cuanto al propósito para el cual la información está siendo colectada.[55]

Limitación del uso, divulgación y retención

Excepto con el expreso consentimiento del individuo o si fuere exigido por ley, la información personal puede utilizarse o divulgarse para los propósitos para los cuales fue colectada. La información personal debe retenerse únicamente por el tiempo necesario para llenar los propósitos identificados o necesarios, y para permitir que la persona pueda acceder a la información después que se haya tomado la decisión. Las organizaciones deben desarrollar lineamientos e implementar procedimientos sobre la retención y destrucción de la información.[56]

Precisión

La información personal utilizada por las organizaciones, inclusive la información divulgada a terceras partes, debe ser precisa, completa y actualizada de acuerdo a las necesidades exigidas para su identificación, especialmente cuando existe un interés del individuo. Los límites de la precisión de la información debe establecerse claramente. La información personal no debe ser actualizada rutinariamente a menos que se precise para los propósitos para los cuales se colectó la información.[57]

Salvaguardias

Las salvaguardias de seguridad deben estar en posición para proteger la información personal contra pérdida, robo, acceso no autorizado, divulgación, copia, uso o modificación. La naturaleza de las salvaguardias debe ser apropiada para la sensibilidad, volumen, distribución, formato y almacenamiento de la información. Los métodos de protección deben incluir medidas físicas, tales como cerrar con llave los archivos, tomar medidas organizacionales tales como la aprobación de la seguridad, o medidas tecnológicas tales como contraseñas para las computadoras. Los empleados deben estar plenamente conscientes de la necesidad de proteger la confidencialidad de la información personal, y

---

54 LIPDE, Artículo 7; Programa 1, Principio 3.
55 LIPDE, Programa 1, Principio 4.
56 LIPDE, Programa 1, Principio 5.
57 LIPDE, Programa 1, Principio 6.

tomar todos los cuidados necesarios para que, aún manteniendo la información disponible, se evite el acceso no autorizado.[58]

Transparencia

Toda información sobre las políticas y prácticas de una organización que se relacionen a la administración de la información personal debe ser suministrada al público. Dicha información debe incluir el nombre, título y dirección de la persona a cargo del cumplimiento con la Ley y a quien se pueden dirigir las reclamaciones; la descripción de la naturaleza de la información personal que está en manos de la organización; la manera en que se puede obtener acceso a la información; y que tipo de información se suministra a las organizaciones asociadas, por ejemplo, las subsidiarias. Esta información debe ser fácil de obtener y de comprender.[59]

Acceso individual

Los individuos tienen el derecho de acceder su propia información personal, impugnar su veracidad e integridad y exigir que se las corrija. El acceso debe ser otorgado a menos que pueda comprometer los datos personales de otros individuos, sea demasiado caro, o está protegido por razones propietarias de naturaleza legal, de seguridad o comercial, o por el privilegio inherente a la relación cliente-abogado. Las organizaciones deben informar a la persona sobre el tipo de información personal que poseen, cómo la utilizan, y a que terceras partes ha sido divulgadas. La solicitud de acceso a la información debe ser respondida en un período razonable, que generalmente es de 30 días. En el caso que se rechace una solicitud de acceso a la información, el individuo debe recibir una comunicación por escrito conteniendo los motivos y cualquier otro recurso disponible bajo la Ley.[60]

Impugnación del cumplimiento

Los individuos tienen derecho a presentar su reclamación sobre la falta de cumplimiento de la organización respecto a la Ley al oficial designado para ese fin.[61] En el caso que un individuo no pueda resolver una controversia con el oficial designado, él o ella pueden quejarse al Comisionado Federal sobre Privacidad quien desempeña las funciones de un defensor civil (*ombudsman).* El Comisionado de Privacidad recibe las reclamaciones relativas a contravenciones a la Ley, realiza investigaciones, y trata de solucionar las reclamaciones a través de la persuasión, mediación y conciliación. Él o ella tiene el poder de buscar y examinar toda la información pertinente mientras está conduciendo la investigación y puede entrar en las instalaciones ocupadas por la organización, examinar los registros importantes, y entrevistar a los individuos. Después de realizarse la investigación, el Comisionado de Privacidad puede redactar un informe con todos los hallazgos apropiados y sus recomendaciones. Cualquier persona que obstruye la investigación del Comisionado, destruye documentos o tome alguna actitud contra los denunciantes son culpables de una ofensa punible con una multa de $100,000. El Comisionado de Privacidad también puede auditar las prácticas de la administración de la información de una organización y tornar los resultados públicos. La tarea del Comisionado incluye programas de educación pública e investigaciones.[62]

El Comisionado no tiene ningún poder para forzar a la organización de actuar sobre la base de los hallazgos o recomendaciones de un informe. En el caso que una cuestión no se resuelva, sin embargo, un individuo puede presentar una reclamación a la Corte Federal de

---

58 LIPDE, Programa 1, Principio 7.
59 LIPDE, Programa 1, Principio 8.
60 LIPDE, Artículos 8-9; Programa 1, Principio 9.
61 Programa 1, Principio 10.
62 LIPDE, Artículos 11-13. El sitio de la web del Comisionado de Privacidad de Canadá puede encontrase en la siguiente dirección: <http://www.privcom.gc.ca>.

Canadá dentro de los 45 días de haber recibido el informe del Comisionado. El Comisionado puede comparecer en nombre del demandante o como una parte a la audiencia. La Corte puede prescribir medidas correctivas a la organización involucrada y otorgar una indemnización por daños y perjuicios al demandante**,** si fuere apropiado.[63]

2) Otras legislaciones federales

Otras legislaciones del Gobierno canadiense que rigen sobre la protección de la privacidad incluyen el Código Penal que prohíbe la interceptación ilegal de las comunicaciones privadas.[64] Además, también existen leyes sectoriales tales como la Ley de la Banca[65], la Ley de la Compañías de Seguros[66], y de las Compañías de Custodia y Préstamos[67], entre otras, que suministran protección a la privacidad.[68]

3) Quebec: Ley relativa a la protección de la información personal en el sector privado.

La Provincia de Quebec fue la primera jurisdicción en América del Norte a contar con una legislación amplia para regir la protección a la información personal en el sector privado, cuando en 1993 aprobó la *Ley relativa a la protección de la información personal en el sector privado*. La ley regula la colecta, uso y divulgación de la información personal y otorga a los individuos el derecho al acceso a sus datos personales y de solicitar la corrección que se hiciere necesaria. Las demandas pueden presentarse a la Comisión de Acceso a la Información [*Commission d'accès à l'information*].

d) Chile

1) La Constitución chilena y otras leyes

La privacidad y carácter secreto de las comunicaciones se encuentran protegidas bajo el Artículo 19 de la Constitución chilena de 1980. La Ley N° 19. 423 prohíbe la grabación encubierta, la interceptación telefónica, y otros métodos clandestinos. La información obtenida por cualesquiera de estos métodos sólo puede divulgarse por intermedio de una orden judicial.[69]

2) Ley sobre la protección de datos personales

La *Ley sobre la protección de datos personales*[70] de agosto 1999, es la primera ley amplia y comprensible sobre la protección de datos personales aplicable al sector público y privado en América Latina. La Ley regula tanto el procesamiento electrónico como manual de los datos personales. Los principios mencionados a continuación, se encuentran garantizados por esta Ley:

<u>Prácticas equitativas de información</u>

El procesamiento de datos sólo puede ocurrir en concordancia con las prácticas equitativas de la información, reconocidas internacionalmente.

<u>Consentimiento</u>

---

63 LIPDE, Artículos 14-17.
64 Código Penal, c-46, "184, 193.
65 R.S.C. ch. B-101, " 242, 244, 459.
66 R.S.C. ch I-11.8, " 489, 607.
67 R.S.C. ch T-19.8, " 444.
68 Vea David Banisar y Simon Davies, *Op. cit.*, p. 26-30.
69 Vea David Banisar y Simon Davies, *Op.cit.*, p. 30-31.
70 En-línea: *Privacy Exchange, National Omnibus Laws*: <http://www.privacyexchange.org/>.

El procesamiento de datos personales exige el expreso consentimiento por escrito del sujeto a quien pertenecen los datos, a menos que se encuentre autorizada por ley. El consentimiento puede revocarse (pero nunca retroactivamente), por escrito. No existe ningún otro requisito que se exige para obtener consentimiento si los datos se encuentran públicamente disponibles; se utiliza únicamente para propósitos internos; se comparte con asociados o afiliados; o se utiliza por razones estadísticas o de clasificación.

Los datos personales sólo pueden usarse para el/los propósito(s) para el/los cual/cuales han sido colectados. Los individuos pueden oponerse al uso de sus datos personales con fines publicitarios o para encuestas de mercado.

Datos sensibles

Los datos sensibles, inclusive aquellos que dan a conocer información sobre raza, origen étnico, opinión política, creencia filosófica o religiosa, salud física o mental, vida sexual, y hábitos personales, sólo podrán ser procesados si están debidamente autorizados por ley, el individuo ha otorgado su expreso consentimiento para ese fin, o si su procesamiento se hace imprescindible para determinar el tratamiento médico de la persona y ventajas para su salud. La información personal médica sólo podrá hacerse pública con el expreso consentimiento por escrito del paciente.

Precisión y seguridad

Los procesadores de datos deben asegurar que los datos son precisos, están completos, actualizados y seguros.

Acceso y transparencia

Debe informarse a los individuos quién colecta la información personal, qué tipo de información se colecta y para qué fin, y quien es la tercera parte que va a recibir dicha información. Transcurridos seis meses y así sucesivamente, ellos también tienen derecho a recibir una copia gratis de la información que se encuentra en manos de la organización. Además de solicitar la corrección de sus datos personales, los individuos también pueden requerir su bloqueo o eliminación 1) cuando fueron suministrados voluntariamente; 2) son antiguos u obsoletos; 3) están siendo utilizados para fines comerciales.

Ejecución

Aunque no existe ninguna disposición sobre la existencia de una autoridad independiente para la protección de datos, las demandas o recursos pueden presentarse ante las cortes.

Cabe añadir que Chile no cuenta con nueva legislación posterior al informe del Dr. Fried. Puede mencionarse que se han dictado decretos que declaran ciertos actos y documentos municipales como secretos debido a los intereses privados que se encuentran en juego. Tal sería el caso, por ejemplo, del Decreto 779/2000, Prueba el Reglamento del Registro de Bancos de Datos Personales a Cargo de Organismos Públicos.

e) México

1) Constitución mexicana

A pesar que la Constitución mexicana no contiene disposiciones específicas respecto a la revelación de datos electrónicos, lo que sí tiene son Artículos generales que se refieren al derecho a la información y a la libertad de prensa.[71] El Artículo 6 estipula que el derecho

[71] La información sobre la ley federal de México fue suministrada por Heather Jeffrey y Gillian Moran de la Embajada Canadiense en México, el 24 de julio de 2000.

a la información será garantizado por el estado. El Artículo 7 limita la libertad de prensa en lo que atañe a la privacidad, moralidad y a la paz pública.

El Artículo 16 de la Constitución mexicana estipula:

> Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.
> .....
> La autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policía; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetándose, en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos.

2) Legislación

La Ley Federal de Transparencia y Acceso a la Información Pública, publicada el 11 de junio de 2002, contiene un capítulo destinado a la protección de datos personales. Allí se prevé el acceso y la posibilidad de corregir información de carácter personal. Las disposiciones de la Constitución se complementan además con algunas leyes sectoriales, inclusive la *Ley federal del derecho de autor*.

El Artículo 109 de la *Ley federal del derecho de autor*, estipula que es ilegal vender u ofrecer información personal que se encuentre en una base de datos electrónica, sin la autorización del individuo. El texto del Artículo 109 dice:

> *El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.*

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

f) Perú

1) Constitución Política de Perú

La Constitución peruana de 1993 establece en su artículo 2, inciso 5, el derecho a "solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.
El secreto bancario y la reserva tributaria pueden levantarse a pedido del Juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado". El siguiente inciso del mismo artículo consagra además el derecho a "que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".

A su vez, el artículo 200 de la misma ley fundamental instituye como garantía constitucional al habeas data, prescribiendo que la misma "procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza

los derechos a que se refiere el Artículo 2º, incisos 5) y 6) de la Constitución". *(Inciso reformado por Ley Nº 26.470 del 12 de junio de 1995.)*

2) Legislación

El Código Procesal Constitucional (Ley No. 28237), regula desde 2004 el procedimiento de la acción de habeas data. En su artículo 60, el Código establece el derecho a acudir a dicho proceso para acceder a información que obre en poder de cualquier entidad pública, así como a conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas. También se contempla la posibilidad de hacer suprimir o impedir el suministro de datos o información de carácter sensible o privado que puedan afectar derechos constitucionales.

También cabe mencionar la Ley 27489, de junio de 2001, la cual regula las entidades privadas de informacion de riesgos (relacionada con capacidad y trayectoria en endeudamiento y pago) y la protección del titular de la información, así como la promulgación, en abril de 2005, de una ley que regula el uso del correo electrónico comercial no solicitado (spam).

3) Código Penal

Bajo el Artículo 154 del Código Penal peruano "el que viola la privacidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios, será reprimido con pena privativa de libertad no mayor de dos años." El Artículo 151 del Código Penal estipula que "*cualquier persona que ilícitamente abre una carta, documento, telegrama, radiotelegrama, mensaje telefónico u otro documento de naturaleza similar que no esté dirigido a ella, o que ilícitamente toma posesión de cualquiera de estos documentos aún si se encuentra abierto, será sancionada con prisión no mayor de dos años y a una multa equivalente desde 60 hasta 90 días de trabajo.*"g) Estados Unidos

La Constitución de los Estados Unidos no protege explícitamente el derecho a la privacidad. La Corte Suprema opina que un derecho a la privacidad constitucional limitado surge de la Declaración de Derechos con respecto a la vigilancia gubernamental. El derecho a la privacidad en el sector privado sólo se encuentra garantizado cuando existe una legislación pertinente. No existe ninguna autoridad de supervisión de la privacidad en los Estados Unidos. La Oficina de Administración y Presupuesto juega un papel de política en el sector público federal, y la Comisión Federal del Comercio supervisa la información crediticia del consumidor y el uso de prácticas comerciales justas.[72] Estados Unidos no dispone de una ley amplia para controlar el acceso a y la protección de información y datos personales que están en el poder de las organizaciones privadas.[73] En cambio, los Estados Unidos han legislado sobre una base sectorial y dependen considerablemente en la autorregulación del sector privado. La legislación que rige la protección a la privacidad en el sector privado incluye, entre otras, las siguientes leyes:

1) Ley sobre la política de las comunicaciones por cable

La *Ley sobre la política de las comunicaciones por cable*[74] (1984) regula el uso de los registros de los abonados a la televisión por cable. Los consumidores deben informar la naturaleza de la información colectada y su uso. La información identificable, tal como las preferencias del espectador no pueden ser divulgadas sin su consentimiento escrito. La

---

72 Vea David Banisar y Simon Davies, *Op. cit*., p. 108-111.

73 El uso de los datos personales por parte del gobierno federal se encuentra regulado por la Ley de Privacidad [*Privacy Act]* (1974), 5 U.S.C. ' 552a (1994).

74 47 U.S.C. ' 551.

información debe ser precisa y deben existir procedimientos cuanto a las correcciones. Por lo menos una vez al año, los consumidores deben ser notificados sobre la "naturaleza, frecuencia, y propósito" de la información almacenada y divulgada. Mediante una demanda en la Corte pueden obtenerse daños y perjuicios reales y punitorios.

2) Ley de protección de la privacidad en-línea de los niños

La *Ley de protección de la privacidad en-línea de los niños [Children's online privacy protection act*] (1998)[75] se aplica a la información que los niños colectan en-línea. La Ley exige que los padres deben otorgar su consentimiento antes que se colecte o divulgue información sobre niños menores de 13 años.[76] También debe otorgarse acceso a los datos colectados a los padres, quienes pueden prevenir que se continúe usando esta información. Los operadores de *websites* comerciales deben informar a los padres sobre las prácticas que utilizan, así como mantener absoluta confidencialidad, seguridad e integridad de la información.

3) Ley de privacidad en las comunicaciones electrónicas

El uso de comunicaciones electrónicas, inclusive voz, video y comunicación de datos, se encuentra regida por la *Ley de privacidad de las comunicaciones electrónicas* [*Electronic communications privacy act*][77] (1986). La ley prohíbe la interceptación no autorizada, adquisición, o divulgación de comunicaciones electrónicas, inclusive aquellas almacenadas en una computadora, a menos que la comunicación se encuentre fácilmente disponible al público en general. Ella se aplica tanto al sector público como al privado. Sin embargo, la Ley permite varias excepciones. Los operadores de sistemas computarizados, por ejemplo, pueden acceder a los datos almacenados y divulgar la información obtenida accidentalmente, a las autoridades gubernamentales. Visto que el sistema puede configurarse para almacenar todos los mensajes que pasan por él, el operador del sistema puede obtener acceso a todos los mensajes que pasan por el mismo. La violación de comunicaciones privadas conlleva a potenciales daños criminales y civiles.[78]

4) Ley de informes crediticios equitativos

Bajo la *Ley de informes crediticios equitativos* [*Fair credit reporting act]*[79] de 1970, la colecta y uso de informaciones obtenidas por las agencias de informaciones crediticias está debidamente regulada. La Ley se aplica a las actividades de aquellos que suministran la información a las agencias de crédito, a las agencias de crédito en sí, y a los usuarios de la información crediticia. Las agencias de crédito deben asegurar que su información es precisa y suministrar procedimientos correctivos. Sus registros deben permanecer disponibles a los consumidores. La información sólo puede liberarse para los consumidores autorizados quienes deben notificar al consumidor si se ha tomado cualquier tipo de acción adversa sobre la base del informe crediticio. Los usuarios también deben informar al consumidor la fuente de la información crediticia. Si la información está incompleta o es imprecisa, el consumidor puede solicitar que la agencia de crédito investigue el caso sin costo alguno. La Ley está siendo administrada por la Comisión Federal del Comercio que tiene un empoderamiento limitado en el campo procesal, investigativo y de ejecución. Las personas perjudicadas también pueden llevar los casos a la corte e iniciar una acción de demanda por daños actuales y punitivos.

---

75 En-línea: *United States, Federal Trade Commission: "Legal Framework, Statutes Enforced or Administered by the Commission, Statutes Relating to Consumer Protection Mission*" <http://www.ftc.gov/ogc/stat3.htm>.

76 Se encuentran disponibles en el sitio de la web denominado "getNetWise": http://www.getnetwise.org/ información para proteger a los niños que usan la Internet, así como programas de filtro.

77 18 U.S.C. ' 2510-2520, 2701-2709 (1997).

78 Vea: Domingo R. Tan, "*Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*" (1999) 21(4). In: Loyola of Los Angeles International and Comparative Law Journal, 661.

79 15 U.S.C. ' 1681-1681(u); Federal Trade Commission: <http://www.ftc.gov/os/statutes/fcra.htm>.

5) Ley del derecho a la privacidad financiera

La *Ley del derecho a la privacidad financiera* [*Right to financial privacy act*][80] regula la transferencia de registros financieros. En forma general, está prohibido que los bancos divulguen los registros financieros de sus clientes sin recibir una orden judicial. Comúnmente, los individuos reciben la oportunidad de oponerse a dar acceso a los registros financieros a los investigadores federales. Puede solicitarse en los Tribunales una reparación judicial por daños reales y punitivos.

6) Ley de protección a la privacidad del video

El arrendamiento o venta de informaciones por video está protegido bajo la *Ley de protección a la privacidad del video* [*Video privacy protection act*] [81]. La ley prohíbe la revelación de los nombres, direcciones y títulos que el consumidor ha comprado o arrendado. Debe brindarse oportunidad a los clientes para retirarse de cualquier programa de mercadeo. Las partes perjudicadas pueden demandar en los Tribunales.

A pesar del hecho que el Gobierno de los Estados Unidos ha regulado la protección de datos en algunas partes del sector privado, continúan existiendo grandes brechas legislativas, por ejemplo, con respecto a los registros médicos, registros bancarios y la Internet. Existe algún tipo de protección de la privacidad a través de la legislación federal y a en sus tribunales. El acto ilícito contra la privacidad fue adoptado por primera vez en 1905, y actualmente se encuentra disponible en casi todos los Estados como un derecho de acción civil.[82] El enfoque general, sin embargo, permanece defendiendo que el sector privado debe auto-regularse a través de códigos de conducta y las fuerzas de mercado. Existe un número de organizaciones basadas en la industria que han desarrollado códigos de conducta. Estas incluyen, entre otras, el "Consejo de Tecnología de la Información para la Industria" [Information Industry Council]; la "Asociación de Servicios Interactivos" [*Interactive Services Association*]; la "Alianza para Privacidad en-línea [*On-line Privacy Alliance*]; y la Asociación Americana de Electrónica".[83]

h) Uruguay

1) Normativa constitucional

El artículo 28 de la Constitución de Uruguay dispone lo siguiente: "Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieron por razones de interés general". Este artículo debe interpretarse en conjunción con los arts. 7, 72 y 332.

2) Leyes y otros instrumentos normativos

La protección de los datos personales se reguló específicamente en la Ley NE 17.838. Dicho cuerpo legal establece el principio de la necesidad de consentimiento expreso e informado del titular para recabar datos que no sean de carácter comercial y exceptúa de este requerimiento a ciertos datos que revistan este carácter (artículo 4),

---

80 12 U.S.C. sec. 3401 et seq.

81 18 U.S.C. ' 2710. Esta Ley fue aprobada en respuesta a los informes de los medios sobre los registros de arrendamiento de videos de la familia del Juez Robert Bork, durante la audiencia para su nominación a la Corte Suprema.

82 Vea David Banisar y Simon Davies, *Op. cit., p.* 108-111.

83 Sobre las Leyes de los Estados Unidos de protección de datos, vea también: *Organization for Economic Cooperation and Development; Directorate for Science, Technology, and Industry; Committee for Information, Computer and Communications Policy; Working Party on Information Security and Privacy; AInventory of Instruments and Mechanisms Contributing to the Implementation and* Enforcement of the OECD Privacy Guidelines on Global Networks,@ DSTI/ICCP/REG (98)12/FINAL, (19 May 1999) at 47-50.

definiéndolos como “listados cuyos datos se limiten a nombres y apellidos, documento de identidad o registro único de contribuyente, nacionalidad, estado civil, nombre del cónyuge, régimen patrimonial del matrimonio, fecha de nacimiento, domicilio y teléfono, ,ocupación o profesión y domicilio”.

La ley establece de forma expresa y no taxativa que los siguientes datos no son de carácter comercial:

-los datos de carácter personal que se originen en el ejercicio de las libertades de emitir opinión informar,

-los relativos a encuestas, estudios de mercado o semejantes,

-los datos sensibles sobre privacidad de las personas, datos referentes al origen racial y étnico de las personas, así como sus preferencias políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o información referente a su salud física o a su sexualidad y toda otra zona reservada a la libertad individual.

Para estos datos, el principio general es que se requiere la expresa y previa conformidad de los titulares y la información a estos del fin y del alcance del registro en cuestión.

La Ley establece además un mecanismo de habeas data y un órgano de control para el caso de violación de las normas de protección que son aplicables a ambas clases de datos. Establece que toda persona tendrá derecho a entablar una acción efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en registros o bancos de datos públicos o privados y, en caso de error, falsedad o discriminación, a exigir su rectificación, supresión o lo que entienda corresponder.

Todo titular de datos personales que previamente acredite su identificación con el documento de identidad, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico. Asimismo, en caso de corresponder por existir error o falsedad en la información, la persona tiene derecho a solicitar la rectificación, actualización y eliminación de los sus datos. En caso de que el responsable de la base de datos no cumpla con la obligación de rectificación en un plazo establecido en la Ley, el interesado queda habilitado para promover la acción de habeas data.

Por su parte, el art. 694 de la ley 16736 estableció el derecho de acceso a los diversos bancos de datos.

Existe además una variedad de disposiciones sectoriales, entre las que se encuentran las normas sobre secreto bancario (decreto ley 15322), el secreto en el Procedimiento Disciplinario, el Registro de Sumarios, competencia de la Oficina del Servicio Civil de la Presidencia de la República, los arts. 17, 40 y 42 del Decreto 258/92, Decreto 396/03 que refieren a las Historias Clínicas y, las leyes 14005 y 17668, que regulan la donación y trasplante de órganos, estableciendo bancos de datos y el necesario secreto a los efectos de proteger a los donantes. Cabe mencionar además la Ley 16616, que regula el sistema estadístico nacional, la cual consagra expresamente algunos principios que han tenerse presentes con miras a resguardar los principios de privacidad y autodeterminación informativa.

Asimismo, existen normas reglamentarias que establecen el principio de libre flujo de información (art. 14 del Decreto 500/91), el legajo electrónico de los funcionarios de la Administración Central (Poder Ejecutivo), Decreto 385/99 y las formas de almacenamiento de documentos electrónicos, Decreto 83/001.

Finalmente, una acordada Suprema Corte de Justicia 7564 de febrero 2006 regula la protección de los datos personales asentados en las bases de datos de dicho organismo.

3) Código Penal

Desde el punto de vista penal, el Código Penal tipifica la violación de correspondencia escrita y de comunicación telegráfica y telefónica y el conocimiento fraudulento de documentos secretos (arts. 296, 297 y 300).

i) Colombia

El artículo 15 Constitución de Colombia prevé lo siguiente: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. (…)

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley”.

A pesar de la disposición constitucional, en Colombia no existe un cuerpo legal destinado a regular comprensivamente el tema de la protección de datos en el sector privado, aunque existen algunas disposiciones sectoriales dispersas en distintos cuerpos legales, tales como la protección de datos relativos a condiciones médicas o la inviolabilidad de la correspondencia. En el pasado se han presentado además varios proyectos de ley que no fueron aprobados. Para la presente legislatura está prevista la discusión en el Congreso colombiano del proyecto de “Ley Estatutaria en materia de habeas data”, mediante el cual se intentará reglamentar el artículo 15 de la Constitución.

Cabe señalar además el papel activo que ha tenido el Tribunal Constitucional colombiano, el cual ha dictado más de un centenar de sentencias relevantes garantizando el cumplimiento del habeas data y la protección de datos personales, dejando asentados algunos principios jurídicos relevantes.

El Código Penal también prevé la tipificación de conductas tales como la violación ilícita de las comunicaciones y la oferta, venta o compra de instrumentos destinados a interceptar comunicaciones privadas.

j) Paraguay

1) Constitución de 1992

El artículo 135 de la Constitución del Paraguay contempla específicamente la figura del habeas data en los siguientes términos: “Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su

finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos".

2) Legislación

El Paraguay cuenta con una Ley que reglamenta la información de carácter privado, la Ley No. 1682/01, la cual ha sido modificada por la Ley 1969/02. El objeto de esta legislación es el de "regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares ". Las leyes en cuestión consagran además el derecho de toda persona a acceder a los datos que se encuentren en los registros públicos.

La legislación en cuestión establece igualmente las condiciones bajo las cuales pueden ser publicados o difundidos los datos relativos a personas físicas o jurídicas que aludan a su situación patrimonial, solvencia económica, o el cumplimiento de sus obligaciones comerciales y financieras. Las leyes preven específicamente tres supuestos:

-mediante autorización previa y por escrito del afectado, y con relación a deudas no reclamadas judicialmente
-cuando la divulgación obedezca al cumplimiento de disposiciones legales específicas;
-y cuando la información en cuestión conste en fuentes públicas de información.

La ley prevé además la obligación de actualizar los datos que sobre las personas obren en los registros de las personas o entidades que procesan la información, y establece las sanciones correspondientes, las cuales consisten fundamentalmente en la imposición de multas.

3) Código Penal

El capítulo VII del Título I del Libro 2º del Código Penal de Paraguay contiene un serie de disposiciones relevantes al ámbito de la protección de datos, como las que tipifican la lesión a la intimidad de la persona, la violación al derecho a la comunicación y a la imagen, la violación al secreto de la comunicación o la revelación de secretos de carácter privado.

k) Ecuador

1) Constitución

El artículo 94 de la Constitución de Ecuador dispone lo siguiente: "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellas y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional".

A su vez, el artículo 276 de la misma constitución establece como competencia del Tribunal Constitucional el conocimiento "de las resoluciones que denieguen … el hábeas data…".

2) Legislación

La Ley de Control Constitucional de 1997 regula algunos de los aspectos procesales del instituto, en especial en el Título II, Capítulo II. En su artículo 35, se dispone que puede acudirse al habeas data para los siguientes efectos:

-obtener del poseedor de la información que éste la proporcione al recurrente, en forma completa, clara y verídica;
-obtener el acceso directo a la información;
-obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros;
-obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado, o no la ha divulgado.

Puede mencionarse además el artículo 9 de la Ley de Comercio Electrónico, el cual protege la recopilación, cesión, uso y transmisión de datos personales obtenidos por cualquier medio y especialmente a través de bases de datos. La infracción a estas disposiciones es sancionada como delito.

l) Costa Rica

1) Constitución

La Constitución de Costa Rica no contempla específicamente la protección de datos de carácter personal o a la autodeterminación informativa como bien jurídico específico objeto de tutela. El artículo 24 consagra sin embargo el derecho a la intimidad, extendiendo la protección a las comunicaciones y a los documentos privados.

2) Legislación

No existe una regulación legal de carácter general y comprehensiva acerca de la materia, aunque se ha introducido algún proyecto de ley tendiente a regular la misma, por ejemplo, intentando introducir un capítulo adicional sobre habeas data a la Ley de Jurisdicción Constitucional. La Corte Suprema también ha elaborado un proyecto de ley sobre la materia. La protección de datos actualmente se tutela por vía del régimen general de amparo.

m) Guatemala

Los artículos 30 y 31 de la Constitución de Guatemala regulan el tema de la publicidad de los actos administrativos y del acceso a los archivos y registros, aunque se hace mención únicamente de los archivos y registros de carácter estatal. Se han venido presentando desde hace ya algunos años varios proyectos de ley sobre el tema de habeas data y protección de datos personales, en conjunto con el tema del acceso a la información, aunque hasta la fecha no se ha aprobado ninguna ley al respecto.

n) Panamá

En la Constitución de Panamá no existe un precepto especialmente dedicado al habeas data. La Ley 6 del 22 de enero de 2002 regula, junto con la transparencia en la gestión pública, el habeas data, aunque éste procede únicamente ante las entidades públicas o privadas que en virtud a una concesión brinden servicios públicos. La ley establece el derecho de los perjudicados a la corrección o eliminación de la información incorrecta o desactualizada. La ley 25 de mayo de 2002 se ocupa igualmente de regular el servicio de información en materia de solvencia de crédito, y contiene algunas disposiciones destinadas a reglar la actividad de las entidades que se dediquen a recolectar datos sobre la solvencia económica o el historial de crédito de las personas.

o) Venezuela

1) Constitución de Venezuela

El artículo 28 de la Constitución de 1999 alude expresamente a la protección de datos personales: “Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley”.

El artículo 60 consagra igualmente la protección del honor, la vida privada, la intimidad, la propia imagen, la confidencialidad y la reputación, disponiendo además que la ley podrá limitar el uso de la informática a efectos de garantizar el honor y la intimidad personal y familiar de la ciudadanía.

Finalmente, el artículo 281, numeral 3, atribuye al defensor del pueblo la facultad de interponer la acción de habeas data.

2) Legislación

La Ley especial contra los Delitos Informáticos contiene en su Capítulo III una serie de disposiciones relativas a la privacidad de las personas y de las comunicaciones, los cuales tipifican como delito la conducta realizada en violación de estos bienes jurídicos.

II. REGULACIÓN DEL FLUJO DE DATOS TRANSFRONTERIZO

1. Antecedentes

Tal cual ocurre con muchas transacciones internacionales, el flujo de datos personales a través de las fronteras por medios electrónicos, especialmente la Internet, crea un gran número de cuestionamientos jurisdiccionales. La identificación, asignación y aplicación de la jurisdicción puede provocar bastantes dificultades. El ejemplo dado a seguir puede ilustrar el problema: la información financiera personal sobre un individuo en el País A fue colectada por la Oficina de Crédito. Esta información se almacenó en una computadora del País B así como en su matriz en el País C. El individuo no tenía motivos para sospechar que parte de la información podía estar incorrecta y desea acceder a ella. Las leyes del País A otorgan el derecho a acceder a este tipo de información si se encuentra guardada en el País A. En este caso particular, sin embargo, la información no está almacenada en el País A. El País B tiene una ley similar pero sólo se aplica al sector público y, consecuentemente, excluye cualquier recurso contra la Oficina privada de crédito. El País C también tiene leyes de protección de datos, pero ellas se aplican únicamente a sus propios ciudadanos. No se puede presentar ningún recurso porque el individuo no es un ciudadano del país C. Por consiguiente, a pesar que los tres países tienen leyes para la protección de datos, y la falta de una jurisdicción no permite que el individuo bajo referencia presente un recurso.[84]

[84] “*Conflicting Assertions of National Jurisdiction over Information Matters*.” Anotaciones para un discurso pronunciado por J.T. Fried ante la *Media and Communications Law Section* de la Asociación Canadiense del Colegio de Abogados, Ottawa, 11 de octubre de 1984.

El establecimiento de una norma jurisdiccional para cubrir los sitios en la Internet es algo bastante difícil de lograr, sin crear algún tipo de disputa, debido al hecho que tantos individuos pertenecientes a tantas comunidades distintas utilizan la Internet. También existen problemas adicionales creados por la tecnología, por ejemplo, cuando se trata de determinar quien debería regular un proveedor de Internet específico. Un enfoque podría ser el de asignar jurisdicción de acuerdo al país donde se encuentra registrado en nombre del dominio. Por otra parte, los websites podrían registrarse bajo varios dominios tales como el dominio ".com", así como el dominio ".uk". La jurisdicción basada en el número IP también es difícil de utilizar, porque dos websites distintos podrían usar el mismo número IP. Hasta el establecimiento de la jurisdicción basada en la localidad física del servidor es problemática. Esta política podría estimular la ubicación de los servidores en localidades donde las leyes son más favorables a los propietarios, una especie de refugio-cibernético. De todos modos, es bien probable que cualquier afirmación de una jurisdicción sobre la base de la configuración actual de las tecnologías de la Internet podría quedar condenadas a medida que la tecnología continúe evolucionando.[85]

La globalización del procesamiento de datos torna la protección de la privacidad en una tarea crecientemente más difícil, sin la aplicación de una jurisdicción extraterritorial. Bajo el derecho internacional tradicional, sin embargo, la mayoría de los Estados se oponen a la aceptación de medidas extraterritoriales, que contradicen o debilitan las leyes o políticas nítidamente enunciadas de otro Estado que está ejerciendo la jurisdicción territorial concurrente sobre la misma conducta.[86] Posiblemente puede existir la necesidad de encontrar nuevas formas para tratar de temas relacionados a la jurisdicción del Estado, de enfrentar los retos impuestos por la Internet y otras redes globales. Tanto en el nivel internacional como el doméstico, ya se probaron algunas tentativas para tratar del tema del flujo transfronterizo de datos, inclusive desde el aspecto jurisdiccional.

2. Instrumentos internacionales

Las cuestiones inherentes a la jurisdicción, flujo transfronterizo de datos y la cooperación internacional, han sido tratadas en una manera limitada y generalizada por los Lineamientos OCDE, en la Convención del Consejo de Europa, y en los Lineamientos UE. Un enfoque más detallado del flujo transfronterizo de datos fue adoptado en la Directiva de la UE.

a) Lineamientos de la OCDE

Los Lineamientos de la OCDE suministran algunos principios básicos que tratan sobre el flujo de los datos personas a través de las fronteras y las restricciones legítimas que existen con el propósito de proteger la información. Los Lineamientos recomienda que un país no debe escatimar esfuerzos para asegurar que el flujo transfronterizo de los datos personales "no sufren interrupciones y son seguros". El país "debe evitar las restricciones al flujo transfronterizo de datos personales" a menos que la re-exportación de datos podría circunvenir su legislación nacional sobre privacidad o los otros países no ofrecen "una protección equivalente." Los Lineamientos de la OCDE refuerzan que "los países deben evitar el desarrollar leyes, políticas y prácticas en nombre de la protección de la privacidad de las libertades individuales, que podrían crear obstáculos al flujo transfronterizo de los datos personales que excederían los requisitos que existen para esta protección."[87]

Los Lineamientos de la OCDE fomentan la cooperación internacional al asegurar que "los procedimientos para el flujo transfronterizo de los datos personales y para la protección

---

85 Para discutir sobre la jurisdicción de la Interne en el contexto de las Convenciones europeas, ver: Agne Lindberg, Delphi Lawyers, "*Jurisdiction on the Internet: European Conventions*," 7 de enero de 1998, en el sitio de la web Privacy Exchange, Presentaciones de Conferencia y Ponencias. <http://www.privacyexchange.org/>.

86 Para discutir los principios de la jurisdicción vea:: Pierre Trudel, "*Jurisdiction over the Internet: A Canadian* Perspective" (1998) 32(4) International Lawyer 1027 at 1029-1047.

87 Lineamientos de la OCDE, Parte Tres.

de la privacidad y libertad individual son simples y compatibles con aquellos de los otros Estados miembros". "Se solicita a los Miembros de intercambiar informaciones relacionadas a los Lineamientos y de facilitar "asistencia mutua en todos los asuntos procesales e investigativos involucrados." Finalmente, los países deben desarrollar "principios, domésticos e internacionales, para regir la ley aplicable en el caso del flujo transfronterizo de los datos personales."[88]

b) La Convención del Consejo de Europa

La Convención del Consejo de Europa declara que una [a] Parte no puede, por el único propósito de proteger su privacidad, prohibir o someter a una autorización especial el flujo transfronterizo de datos personales enviados al territorio de otra Parte. Sin embargo, una Parte de la Convención puede bloquear el flujo transfronterizo de datos "en la medida en que su legislación incluye normas específicas para ciertas categorías de datos personales o de archivos personales automatizados, porque la naturaleza de esos datos o archivos, excepto cuando las normas de la otra Parte le otorgan la misma protección." En forma similar, una Parte puede prohibir la transferencia transfronteriza de datos personales cuando "esta transferencia se efectúe desde su territorio al territorio de un Estado no contratante a través de un intermediario del mismo territorio de otra Parte, con el propósito de evitar que dichas transferencias lleguen a circumvenir la legislación..."[89] En otras palabras, la transferencia de datos puede ser bloqueada a países que no ofrecen el mismo nivel de protección.

Para facilitar el flujo transfronterizo de datos, la Convención exige que cada Parte designe una autoridad protectora de datos que suministrará información sobre sus leyes y procedimientos administrativos en el campo de la protección de los datos a las otras Partes.[90] Además, cada Parte debe ayudar a las personas residentes en el extranjero a ejercer sus derechos.[91] La Convención establece un Comité Consultivo que representará a los Estados miembros y elaborará propuestas relativas a la aplicación y mejoría de la Convención.[92]

El proyecto de Protocolo preparado por el Comité Consultivo exige la cooperación de las autoridades supervisoras creadas bajo el Protoclo, como parte del cumplimiento de sus funciones, especialmente a través del intercambio de información.[93]

El Protocolo también trata la cuestión del flujo transfronterizo de datos a un receptor que no es sujeto de la jurisdicción de una Parte de la Convención. También declara que dicha transferencia de datos personales está permitida "únicamente si el Estado de la organización asegura que existe un nivel de protección adecuado para los datos que se pretende transferir."[94] Están permitidas algunas excepciones a esta norma:

a) en el caso que la ley nacional disponga al respecto, debido a intereses específicos del sujeto a quien pertenece la información, o por la prevalencia de intereses legítimos, especialmente cuando se trata de intereses públicos importantes, o

b) en el caso que las salvaguardias, que pueden resultar específicamente de las cláusulas contractuales, provienen del *controller* responsable por la transferencia, siendo consideradas

---

88 Lineamientos de la OCDE, Parte Cinco.
89 Convención del Consejo de Europa, Artículo 12.
90 Convención del Consejo de Europa, Artículo 13.
91 Convención del Consejo de Europa, Artículo 14.
92 Convención del Consejo de Europa, Artículo 18-20.
93 Proyecto de Protocolo, Artículo 1.
94 Proyecto de Protocolo, Artículo 2.

adecuadas por las autoridades competentes de concordancia con la ley nacional. [95]

Las disposiciones del proyecto de Protocolo relativas a la transferencia de datos personales a un tercer país son similares a aquellas que constan en la Directiva de la UE.

c) Lineamientos de las Naciones Unidas

Los Lineamientos de las Naciones Unidas abordan la cuestión del flujo transfronterizo de datos en su Artículo 9, que dice:

> *When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.*

Tal cual ocurren en los Lineamientos de la OCDE, las limitaciones al flujo transfronterizo de datos sólo están permitidas si los estándares de protección a la privacidad exigidos no se cumplen. Deben tomarse medidas para asegurar la protección adecuada a la protección necesaria.

d) Directiva de la Unión Europea sobre la privacidad

Uno de los mayores objetivos de la Directiva de la UE se orientó al flujo transfronterizo de los datos personales y a crear un mercado común europeo. El Artículo 1(2) de la Directiva de la UE determina que los países de la Unión Europea "no podrán restringir ni prohibir la libre circulación de datos entre los Estados miembros." Considerando que todos los Estados de la UE deben suministrar aproximadamente el mismo nivel de protección para los datos personales como resultado de la Directiva de la UE, las limitaciones al libre movimiento de datos meramente por razones de protección de la privacidad no están permitidas dentro de la Unión.

El Capítulo IV de la Directiva de la UE trata sobre la "Transferencia de datos personales a terceros países". Los países de la UE deben bloquear la transferencia de información personal a países que no son Estados miembros que no pueden ofrecer un nivel de protección "adecuado" El Artículo 25 de la Directiva UE, dice:

> *1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.*
>
> *2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos: en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las*

95 Proyecto de Protocolo, Artículo 2.

> *normas de Derecho, generales y sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.*

Las decisiones sobre el grado de adecuación que tiene el régimen de protección de datos de un tercer país se toman primero, bajo la Directiva UE, al nivel de las autoridades nacionales. Los Estados miembros de la UE y la Comisión Europea deben compartir informaciones entre sí sobre casos en los cuales un país tercero no protege correctamente los datos personales.[96] Si la Comisión descubre que el tercer país no ofrece un nivel de protección adecuado, los Estados miembros de la UE deben evitar la transferencia de los datos personales.[97]

El Artículo 26 de la Directiva UE menciona las siguientes excepciones a la regla que indica que los datos personales no pueden transferirse a países que no disponen de un nivel de protección adecuado:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado o,

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero; o

d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

La transferencia de datos personales a un país tercero que no provee una protección adecuada a la privacidad también se permite cuando el responsable indica que existen salvaguardias para proteger la privacidad", por ejemplo, a través de "cláusulas contractuales apropiadas".[98]

Cuando un tercer país no otorga suficiente protección para la privacidad, la Comisión puede iniciar negociaciones "con el propósito de remediar la situación".[99] Dada la importancia de la UE en el marco del intercambio global de información, la Directiva UE puede ejercer consecuencias bastante poderosas fuera de la Unión. Cuando los países terceros no otorgan suficiente legislación para proteger los datos personales en el sector privado, las autoridades públicas o hasta los negocios individuales pueden encontrarse forzados a realizar negociaciones con la Comisión, con el propósito de demostrar su concordancia con las normas de la UE.

---

96 Directiva de la UE, Artículo 25 (3).
97 Directiva de la UE, Artículo 25 (4).
98 Directiva de la UE, Artículo 26.
99 Directiva de la UE, Artículo 25(5).

La Directiva UE fomenta la cooperación transfronteriza entre la Unión Europea estipulando que una "autoridad nacional puede solicitar el ejercicio de su poder por una autoridad de otro Estado miembro" y que las "autoridades supervisoras van a cooperar entre sí cuanto fuere necesario para el desempeño de sus deberes, especialmente mediante el intercambio de informaciones útiles."[100]

3. Legislación nacional

La mayoría de los Estados no tienen una legislación específica que trata sobre el flujo transfronterizo de los datos personales. Sin embargo, las leyes que amparan la protección de datos de algunos países exigen que la liberación de datos personales a Estados extranjeros puede ocurrir únicamente si se cumplen ciertas condiciones. Generalmente, el estado extranjero o la organización receptora debe garantizar un mínimo nivel de protección a la privacidad. Algunas leyes también toman medidas para la cooperación con otras leyes o autoridades que aplican la protección de datos.

a) Argentina

Argentina no dispone de leyes específicas que regulen el flujo de datos en formato electrónico a través de sus fronteras internacionales.[101] No obstante, el Proyecto de Ley N° 606 de 1998 proponiendo el *habeas data,* debidamente aprobado por el Senado argentino prohíbe la transferencia de datos personales de cualquier tipo a otros países o a entidades internacionales o supranacionales que no disponen de un nivel de protección adecuado. La excepción de esta regla es el intercambio de datos con el propósito de ofrecer cooperación jurídica internacional, datos médicos si el tratamiento del paciente lo exige, o durante el curso de una investigación epidemiológica, transferencia bancaria o de acciones, cuando la transferencia se realiza de acuerdo a los tratados internacionales de los cuales Argentina es signataria, o cuando es parte de una cooperación internacional establecida entre agencias de inteligencia con el propósito de luchar contra el crimen organizado, terrorismo y el narcotráfico. No queda bien claro, sin embargo, cómo se aplicará esto a las operaciones internas de corporaciones transnacionales, o a las operaciones de transacciones al nivel comercial.

b) Canadá

La *Ley de privacidad* de Canadá (*Privacy Act*), que se aplica al sector público dispone (en su Artículo 8) sobre la divulgación transfronteriza de la información personal:

> f) *under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;*

Contrariamente a lo que ocurre con la *Ley de privacidad*, la *Ley de información personal y documentos electrónicos* [*Personal information and electronic documents act*] no trata el tema del flujo transfronterizo de la información o cooperación en términos específicos, pero las organizaciones no Canadá continuarán siendo consideradas responsables por la protección adecuada de los datos personales aún cuando los datos se transmiten a través de las fronteras (principio de responsabilidad).[102] En su Sección 17, la *Ley de respeto a la protección de la información personal en el sector privado* de Quebec

---

100 Directiva de la UE, Artículo 28.

101 La información sobre la legislación que rige el procesamiento electrónico de los datos personales en la Argentina, fue suministrada el 26 de julio de 2000, por Hartmuth Kroll, de la Embajada de Canadá en ese país.

102 Discusión con Ken Huband, Política de Privacidad, Industria de Canadá, el 1° de agosto de 2000.

respecting the protection of personal information in the private sector] dispone que al comunicar datos fuera de Quebec, una empresa debe tomar medidas razonables para asegurar que los datos serán utilizados únicamente para el propósito especificado, y que el interesado recibe la oportunidad de objetar al uso de los datos para la búsqueda de clientes.

III. ENFOQUES SOBRE LA PROTECCIÓN DE DATOS

1. Estándares comunes para la protección de datos

Un enfoque que ha sido tomado por los Estados en el ámbito internacional consiste en el acuerdo sobre un nivel mínimo de convergencia sobre los regímenes de protección nacional de datos. La Unión Europea ha asumido el enfoque más decisivo al requerir de sus Estados miembros que armonicen su legislación sobre protección de datos. No obstante que las leyes nacionales no necesitan ser idénticas según la Directiva de la Unión Europea, es necesario que los países alcancen niveles razonablemente altos a fin de crear un mercado común europeo para el flujo de datos. Por otro lado, una organización supranacional, la Comisión Europea, continúa desempeñando un papel importante y coordinador y asegura que los estándares de la Unión no se encuentran minados por transferencias de datos para otros países que no cumplen con los niveles requeridos. Al mismo tiempo que muestra un desafío significativo, este tipo de armonización legislativa puede extenderse más allá de la Unión Europea por medio de tratados bilaterales o convenciones multilaterales.[103]

En realidad, todos los instrumentos internacionales discutidos anteriormente han tratado de estimular la promulgación de leyes que brinden un nivel consistente y comparable de protección a la privacidad en el área del procesamiento de datos personales. Mientras que los lineamientos de la OCDE y los Lineamientos de las Naciones Unidas representan recomendaciones no vinculantes sobre las cuales erigir regímenes de protección de datos, la Convención del Consejo de Europa y particularmente la Directiva de la UE constituyen instrumentos legalmente vinculantes que requieren que los Estados adopten leyes que establezcan un nivel mínimo de protección privada. Como resultado de la Convención del Consejo de Europa y la Directiva de la UE sobre Privacidad, la mayoría de los Estados europeos introdujeron regímenes de protección a la privacidad.[104]

La esperanza que tenemos es que por medio del acuerdo sobre los principios sobre la protección mínima brindada a los datos, los Estados no se vean en la necesidad de imponer restricciones a los flujos de datos que transponen las fronteras. Los instrumentos internacionales mencionados anteriormente contienen limitaciones al libre flujo de datos solamente en ciertos casos excepcionales. Los Lineamientos de la OCDE hacen referencia a países que no “obedecen substancialmente” a tales pautas o dejan de brindar “protección equivalente”: Los Lineamientos de las Naciones Unidas hacen referencia a la falta de “salvaguardias comparativas”. La Convención del Consejo de Europa reclama sobre la ausencia de “protección equivalente” y la Directiva de la UE impone restricciones sobre flujos de datos fuera de la Unión donde terceros países no ofrecen un “nivel adecuado de protección”.

---

[103] La propia directiva de la EU fue negociada bajo la amenaza de un secuestro de datos por parte de ciertos miembros que tenían leyes de protección a datos, inclusive Francia y Alemania, contra aquellos con leyes menos rigurosas, como Italia. La posible interrupción del libre flujo de datos se evitó a través de la elaboración de un conjunto de normas de protección similares. Gregory Shaffer, *Globalization and Social Protection: the impact of EU and international rules in the ratcheting up of U.S.Privacy Standards*, (2000)25(1). In: *Yale Journal of International Law*, p. 1-10.

[104] Para una discusión sobre los regímenes de protección a la privacidad de los países de la OCDE, vea: Directorado de Ciencias; Tecnología e Industria; Comité de la Información; Política de la Tecnología de la Información y Comunicaciones; Grupo de Trabajo de Seguridad y Privacidad de la Información; “*Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks*”, DSTI/ICCP/REG (98)12/FINAL, (19 May 1999).

En los casos en que el nivel requerido de protección está ausente, pueden aplicarse ciertas medidas limitadas de control. Los Lineamientos de la OCDE desestiman medidas que "en nombre de la protección de la privacidad y de las libertades individuales que excederían de requisitos para tal protección". Los principios de las NU recomiendan que las restricciones sean impuestas "hasta el punto que así lo exija la protección de la privacidad". La Convención del Consejo de Europa y la Directiva de la UE brindan claramente un freno al movimiento de informaciones o datos personales hacia los países donde no se asegura protección suficiente.

La Directiva de la UE impone las limitaciones más fuertes al flujo de datos entre fronteras. El Artículo 25 de la Directiva de la UE obliga, más que permite, que los Estados miembros de la UE prohiban la transferencia de información o datos personales a los Estados que no brindan niveles adecuados de protección. El estándar requerido por los Lineamientos de la OCDE y la Convención del Consejo de Europa puede ser más exigente, dado que se refiere a la "equivalencia" más que a la "adecuación", pero la transferencia de datos sólo puede bloquearse de acuerdo a la Directiva de la UE cuando no se lleguen a alcanzar los estándares estipulados. Debido a la importancia económica de la UE, el potencial de tal medida preventiva sobre los datos es un poderoso incentivo para los Estados de todo el mundo para que adopten alguna medida para la armonización en la protección de los datos personales.[105] Allí donde el flujo de datos entre fronteras se ve interrumpido debido a que otro país posee leyes inadecuadas para la protección de la privacidad, se requiere que la Comisión Europea entre en negociaciones con dicho país.

2. Principios de seguridad portuaria

En virtud de la entrada en vigencia de la Directiva de la UE el 25 de octubre de 1998, la Comisión Europea y el Departamento de Comercio de los UE iniciaron negociaciones a fin de evitar la interrupción del libre flujo de datos entre Europa y los Estados Unidos. A fin de disminuir la incertidumbre cuanto al hecho de saber si las organizaciones de la UE pasarían la prueba relativa al "estándar adecuado" con referencia a la protección de datos requerida por la Directiva de la UE, los Estados Unidos propusieron que las compañías norteamericanas que quisieran recibir datos personales provenientes de la Unión Europea adhiriesen a los denominados "Principios de seguridad portuaria.[106] La adhesión a dichos Principios establecería una "presunción sobre una adecuada protección de la privacidad" con referencia a los propósitos de la Directiva de la UE.

La decisión de una organización para adherirse a los *Principios de seguridad portuaria* es voluntaria. Las organizaciones pueden adherirse a los Principios de diversas maneras. Pueden adoptar un programa conjunto sobre la privacidad que siga los Principios o pueden poner en práctica sus propias políticas auto-regladas, siempre que obedezcan a los principios. Si una organización deja de cumplir con la autorregulación, puede ser demandada según la Sección 5 de la Ley de *Comisión de Comercio Federal,* que prohíbe "los actos desleales y fraudulentos". Las organizaciones sujetas a leyes, reglamentos o normas administrativas que efectivamente protegen la privacidad pueden también adherirse a los *Principios de seguridad portuaria*. A fin de hacerlo, las organizaciones deben certificar por ante el Departamento de Comercio sobre su adhesión a los Principios de acuerdo con las pautas descriptas en las *Preguntas más frecuentes*.

---

[105] Por ejemplo, los efectos extraterritoriales en potencial resultantes de la Directiva de la UE han estimulado a los países no europeos como Canadá, Hong Kong, Nueva Zelandia y Taiwan de promulgar una legislación sobre la protección de los datos para cubrir al sector privado. Vea: Comisionado de Privacidad, Nueva Zelandia, *"Report by the Privacy Commissioner to the Minister of Justice on the Trans-Tasman Mutual Recognition Bill and Transborder Data Flows*," Comisionado de Privacidad, Nueva Zelandia, *"Reports and Submissions*": <http://www.privacy.org.nz/people/transtas.html>.

[106] Departamento de Comercio de los EE.UU., "*Safe Harbour Principles*" (21 julio de 2000), online: *Privacy Exchange, News*: <http://www.privacyexchange.org/>. Vea también en-línea: *Europa, European Commission, Internal Market, Media Information Society and Data Protection, Data Protection, News,* <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm>. "Anexo al Principio de Seguridad Portuaria": Privacy Exchange, News: <http://www.privacyexchange.org/>.

Los *Principios de seguridad portuaria* según su versión final del 21 de julio de 2000 son los siguientes:

"Datos personales" e "información personal" son los datos sobre un individuo identificado o identificable que se encuentran dentro del alcance de la Directiva, recibidos de la Unión Europea por una organización de los UE y registrados de alguna manera.

NOTA: La organización debe informar a los individuos sobre los propósitos para los cuales recoge y utiliza información sobre ellos, como contactar a la organización sobre cualquier pregunta o queja, los tipos de terceros a los cuales revela la información, y las alternativas y medios que la organización ofrece a los individuos para limitar dicho uso y revelación. Esa nota debe ser brindado en lenguaje claro y conspicuo cuando se requiere que los individuos, por primera vez, brinden información personal a la organización o tan pronto como sea posible, pero en cualquier caso antes que la organización utilice dicha información para un propósito que no sea aquél para el cual fue originalmente recogida o procesada por la organización que la transfirió o que la revela por primera vez a un tercero (1).

ELECCIÓN: Una organización debe ofrecer a los individuos la oportunidad de escoger si su información personal (a) puede revelarse a terceros (1) o (b) puede utilizarse con un propósito que es incompatible con el o los propósitos para los cuales fue originalmente recogida o subsecuentemente autorizada por el individuo. Los individuos deben contar con mecanismos claros y conspicuos, rápidamente disponibles y a su alcance para efectuar la elección.

Para la información de carácter sensible (por ejemplo, información personal que especifique condiciones médicas o de salud, orígenes étnicos o raciales, opiniones políticas, creencias religiosas o filosóficas, participación en sindicatos de comercio o información relativa a la vida sexual del individuo) deben ser brindadas opciones afirmativas o explícitas en caso de que la información deba ser revelada a terceros o utilizada para un propósito distinto de aquel para el cual fue originalmente recogida o subsecuentemente autorizada por el individuo por medio del ejercicio de su elección. En cualquier caso, toda organización debería tratar como sensible cualquier información recibida de un tercero cuando dicho tercero la trata e identifica como tal.

TRANSFERENCIA: a fin de revelar la información para un tercero las organizaciones deben aplicar los Principios sobre Comunicación y Elección. Cuando una organización desea transferir la información a un tercero que está actuando como agente, tal como se describe en la nota final, puede hacerse si primeramente comprueba que el tercero adopta los Principios o se halla sujeto a la Directiva u otra medida adecuada, o concuerda por escrito con dicho tercero requiriendo que dicho tercero brinde al menos el mismo nivel de protección a la privacidad como el requerido por los Principios relevantes. Si la organización cumple con estos requisitos, no será responsabilizada (a menos que la organización lo considere de otra manera) cuando un tercero al cual transfiere dicha información la procesa de manera contrario a cualquier restricción o manifestación, a menos que la organización supiese o debiera haber sabido que el tercero la procesaría de manera contraria y que la organización no ha tomado las medidas adecuadas para prevenir o hacer cesar tal procesamiento.

SEGURIDAD: Las organizaciones que crean, mantienen, utilizan o divulgan información personal deben tomar precauciones razonables a fin de protegerlas contra la pérdida, uso indebido o acceso no autorizado, revelación, modificación y destrucción.

INTEGRIDAD DE LOS DATOS: Consistente con los Principios, la información personal debe ser relevante para los propósitos para los cuales es utilizada. Una

organización no debe procesar información personal de tal manera que sea incompatible con los propósitos para los cuales ha sido recogida o subsecuentemente autorizada por el individuo. En la medida necesaria para tales propósitos, una organización debería adoptar medidas razonables para asegurar que la información es confiable para el uso al cual se destina, correcta, completa y vigente.

ACCESO: Los individuos deben tener acceso a la información personal que sobre ellos posee una organización, y serles posible corregir, alterar o eliminar dicha información cuando la misma sea incorrecta, excepto cuanto el costo o gasto de brindar tal acceso sea desproporcionado a los riesgos para la privacidad del individuo en el caso en cuestión, o cuando los derechos de personas ajenas al individuo pudiesen ser violados.

OBSERVANCIA: La protección efectiva a la privacidad debe incluir mecanismos para asegurar el cumplimiento de los Principios, recursos para los individuos afectados por el incumplimiento de los Principios en lo que hace a la información, y consecuencias para la organización cuando tales Principios no sean observados. Como mínimo, tales mecanismos deben incluir (a) mecanismos independientes de recursos rápidamente disponibles y al alcance por medio de los cuales las quejas de cada individuos y los litigios sean investigados y resueltos mediando referencia a los Principios, y garantizando el pago de daños cuando la ley aplicable o las iniciativas del sector privado así lo disponen; (b) procedimientos para verificar que las certificaciones y las declaraciones que las empresas comerciales hacen sobre sus prácticas privadas son verdaderas y que dichas prácticas han sido implementadas tal como se han presentado; y (c) obligaciones para subsanar problemas derivados de la falta de cumplimiento de los Principios por parte de organizaciones que anuncian su adhesión a los mismos y las consecuencias para tales organizaciones. Las sanciones deben ser suficientemente rigurosas a fin de asegurar el cumplimiento por parte de las organizaciones.

1. no es necesario dar noticia o hacer una elección cuando la divulgación se efectúa a un tercero que actúa como agente para llevar a cabo tarea(s) en nombre y bajo las instrucciones de la organización. El Principio de Transferencia, por otro lado, se aplica a tales casos.

Estos Principios se complementan con un documento que trata de las *Preguntas más frecuentes*, brindando una guía para la interpretación de los Principios.[107]

La adhesión a los Principios puede ser limitada por lo siguiente:

a) en la medida necesaria para proteger la seguridad nacional, el interés público, o los requerimientos para la observancia de la ley;

b) por normas, reglamentos gubernamentales o ley casuística que crean obligaciones conflictivas o autorizaciones explícitas, siempre que, al ejercitar tal autorización, una organización pueda demostrar que su incumplimiento para con los principios se limita a la medida necesaria a fin de cumplir con intereses legítimos favorecidos por tal autorización; o

c) si el efecto de la Directiva o de la Ley del Estado miembro es permitir excepciones o derogaciones, siempre que las mismas sean aplicables en contextos comparativos.

La Unión Europea reconoce que la Comisión Federal de Comercio y el Departamento de Transporte de los UE “poseen facultades para investigar las quejas y obtener alivio contra prácticas desleales o fraudulentas así como reparaciones a individuos en caso de

[107] En línea: Intercambio de Privacidad, Noticias. http://www.privacyexchange.org/>.

incumplimiento de los principios implementados de acuerdo con las *Preguntas más frecuentes*.[108]

Aunque la Comisión Europea ya ha aceptado la "adecuación" de los *Principios de seguridad portuaria*[109], el Parlamento Europeo requirió la imposición de requisitos adicionales el 14 de julio del 2000:[110]

- reconocimiento de un derecho individual de apelación a un cuerpo público independiente facultado para considerar cualquier recurso relacionado con una violación alegada de los Principios;
- obligación de que las firmas participantes compensen los daños, sean morales o causados a la propiedad, que han sufrido aquellos que se encuentren involucrados, en el caso de violaciones contra los Principios, y un compromiso asumido por las firmas a fin de cancelar la información personal obtenida o procesada de manera ilegal;
- facilidad de identificación de las medidas a ser tomadas a fin de asegurar que los datos sean cancelados y obtener compensación por cualquier daño sufrido;
- disponibilidad de un chequeo preliminar por parte de la Comisión sobre el funcionamiento adecuado del sistema dentro de los seis meses de su entrada en vigor y presentación de un informe sobre el resultado del chequeo y de cualquier problema encontrado en la parte actuante según el Artículo 29 y el Comité según el Artículo 31 de la Directiva, así como sobre el comité relevante del Parlamento Europeo;

A pesar de estas preocupaciones por parte del Parlamento Europeo, la Comisión Europea emitió una Decisión el 27 de julio del 2000, aceptando los *Principios de seguridad portuaria* expedidos por el Gobierno de los Estados Unidos el 21 de julio del 2000.[111] La Comisión decidió proseguir con la Decisión, dado que el Parlamento Europeo no había encontrado que la Comisión, al así hacerlo, estaría excediendo sus facultades. No obstante, La Comisión notificó al Departamento de Comercio de los UE sobre las preocupaciones del Parlamento Europeo y declaró que reabriría las discusiones en caso de que los temores del Parlamento relativos a lo inadecuado de los recursos disponibles para los individuos demostrasen poseer bases sólidas.

3. Asistencia mutua y cooperación

Cuando los países no pueden concordar sobre el establecimiento de un régimen común de protección de datos por medio de la armonización legislativa u otros mecanismos tales como los *Principios de seguridad portuaria*, la efectividad de la legislación nacional puede no obstante ser incrementada por medio de acuerdos de asistencia mutua y cooperación. A fin de aplicar las leyes de protección de datos, los órganos adjudicativos deben estar capacitados a ejercitar algún control o influencia sobre los infractores y obtener las pruebas necesarias. Particularmente en el área de protección de la información personal en la Internet y otras redes globales, se requiere la cooperación internacional dado que los países individualmente considerados no pueden tratar este asunto. Algunos de los instrumentos internacionales discutidos más arriba así como las leyes nacionales brindan

---

108 "*Annex to the Safe Harbour Principles",* en línea: Intercambio de Privacidad, Noticias http://www.privacyexchange.org/>.

109 Decisión de la Comisión C5-0280/2000.

110 "Resolución del Parlamento Europeo sobre el proyecto de Decisión de la Comisión relativa a determinar si la protección suministrada por los Principios de Privacidad de la Seguridad Portuaria es adecuada, y está relacionada a las *Preguntas más frecuentes* emitidas por el Departamento de Comercio de los EE.UU. (C5-0280/2000 - 2000/2144 (COS)) en "Acta del 05/07/2000 – Edición Provisional " en el sitio de la web de la Unión Europea, Parlamento Europeo, Búsqueda de Guías, Resoluciones*;* <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm>.

111 "Protección de los Datos: La Comisión adoptó decisiones reconociendo que los regímenes en los EE.UU., Suiza y Hungría era adecuados: ", en línea: Europa, Comisión Europea, Mercado Interno, Sociedad de Protección de Datos, y Medios de la Tecnología de la Información Protección de Datos, News, <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm>.

facilidades sobre la cooperación entre las autoridades encargadas de la protección de datos a través de las fronteras internacionales. Las disposiciones sobre asistencia mutua han sido también incluidas en otros tratados bilaterales y multilaterales, especialmente aquellos relativos a la ley penal.[112]

a) Asistencia mutua en los instrumentos internacionales

Los Lineamientos de la OCDE estimulan a los miembros a intercambiar información relacionada con los principios y a facilitar "la asistencia mutua en los asuntos procesales e investigativos".[113] La Convención del Consejo de Europa requiere de cada autoridad de protección de la información de cada Parte que brinde información sobre sus leyes y procedimientos administrativos en el área de protección de datos a otras Partes y a brindar ayuda a las personas que residan en el extranjero a fin de ejercitar sus derechos.[114] La Directiva de los UE estipula que "una autoridad de otro Estado miembro puede requerir a otra autoridad nacional para que ésta que ejercite sus facultades" y que "las autoridades de supervisión deberán cooperar entre sí en la medida necesaria para el cumplimiento de sus obligaciones, en particular mediante el intercambio de información de utilidad." [115]

b) Proyecto de convención sobre delitos cibernéticos

La Convención propuesta sobre delitos cibernéticos es de importancia para la discusión sobre la protección internacional de la información y para la ayuda legal mutua. Dicha convención está siendo actualmente negociada por los Estados miembros del Consejo de Europa y un número de Estados incluyendo Canadá, Japón, Sudáfrica y los Estados Unidos. El Consejo de Europa ha publicado la versión actual del Proyecto de Convención (Proyecto No. 19) en la Internet.[116] Varias disposiciones del Proyecto de Convenio se relacionan directamente con la protección de la información personal, tal como aquellos referidos con el acceso ilegal a los sistemas de computación (Artículo 2); la interceptación ilegal de datos de computador (Artículo 3); la interferencia con información computadorizada (Artículo 4) o con un sistema informático (Artículo 5); u otras violaciones relacionadas al ambiente de computación tal como la falsificación Artículo 7) o el fraude (Artículo 8). Por otro lado, el Proyecto de Convención contiene un lenguaje que puede ser útil al tratar de cuestiones de jurisdicción y asistencia legal mutua. La Convención toca el tema relativo a la jurisdicción en el Artículo 19:

1. Cada miembro tomará las medidas legislativas y de otro tipo que sean necesarias para establecer la jurisdicción sobre cualquier violación…. cuando la violación sea cometida:

a. [total o parcialmente] en su territorio o sobre un navío, aeronave o un satélite portando su bandera o registrado en dicho país Parte;

b. por uno de sus nacionales, si la violación es sancionable según la ley penal del lugar donde se ha cometido o si la violación se ha cometido fuera de la jurisdicción territorial de cualquier Estado …

---

112 Vea por ejemplo: Tratado entre el Gobierno de los Estados Unidos y el Gobierno de Canadá sobre Cooperación Jurídica Mutua en Materia Penal [*Treaty Between the Government of the United States and the Government of Canada on Mutual Legal Assistance in Criminal Matters*] (18 marzo 1985) 24 I.L.M. 1092 y Ley Canadiense sobre Cooperación Jurídica Mutua en Materia Penal [*Canadian Mutual Legal Assistance in Criminal Matters Ac*t], ch. M-13.6 (R.S., 1985, c. 30 (4th Supp.); en-línea: *Canada, Departament of Justice, "Consolidated Statutes"* <http://canada.justice.gc.ca/FTP/EN/Laws/Chp/MM-13.6.txt>.

113 Lineamientos OCDE, Part V.

114 Convención del Consejo de Europa, Artículos 13 & 14.

115. Directiva UE, Artículo 28.

116 Consejo de Europa, Directorado General, I. Asuntos Jurídicos, Oficia de Tratados, "Proyectos de Tratados": <http://conventions.coe.int/treaty/EN/cadreprojets.htm> [de ahora en adelante denominado Proyecto de Convención sobre Delitos Cibernéticos].

5. Cuando más de una Parte reclame jurisdicción sobre una alegada violación establecida de acuerdo con esta Convención, las Partes interesadas, cuando sea apropiado, se consultaran a fin de determinar la jurisdicción más adecuada a fin de proseguir el caso.

El proyecto de Convención estimula claramente a los Estados a declarar su jurisdicción sobre los infractores en su territorio, así como sus nacionales, por medio de las consultas, cuando sea requerido.

El Artículo 20 del Proyecto de Convención describe principios generales relacionados con la cooperación internacional:

Las Partes cooperarán entre sí, de acuerdo con las disposiciones de este capítulo, y por medio de la aplicación de los instrumentos internacionales adecuados sobre cooperación internacional en asuntos penales, acuerdos logrados en base a la legislación uniforme o recíproca, y leyes nacionales, en la mayor medida posible para los fines de las investigaciones y procedimientos relativos a las violaciones penales relacionadas con los sistemas de computación y de datos, o para la obtención de prueba electrónica sobre un delito penal.

Se requiere de los Estados que utilicen cualquier medio legal a fin de perseguir a los infractores.

El Artículo 22 del Proyecto de Convención solicita a las partes que brinden rápida asistencia mutua a los fines de la aplicación y observancia de las normas:

1. Las Partes se brindarán asistencia mutua en la mayor medida posible a fin de realizar investigaciones y procedimientos relativos a las violaciones penales relacionadas con los sistemas de computación y de datos, o para la obtención de pruebas electrónicas sobre una violación penal.

2. A los fines de brindar la cooperación relativa a los Artículos 24-29, cada Parte, en circunstancias de urgencias, aceptará y responderá a los pedidos de asistencia mutua por medios rápidos de comunicación, incluyendo [voz] fax o correo electrónico, en la medida que tales medios proporcionen niveles adecuados de seguridad y autenticidad, seguidos de confirmación formal cuando el Estado requerido así lo exija.

El Proyecto de Convención ofrece procedimientos de asistencia mutua en casos en que no exista tratado de ayuda mutua o acuerdo entre la parte solicitante y los Estados requeridos. Se requiere que cada Parte designe una autoridad central a fin de tratar de los pedidos de asistencia mutua. Debe llevarse un registro de autoridades centrales y las mismas se comunicarán directamente entre sí. La ayuda puede negarse, total o parcialmente, en caso de imposición legal o si la misma pudiese perjudicar la soberanía de la Parte, su seguridad, orden público, u otros intereses esenciales. Las Partes pueden también enviar a las demás, sin pedido previo, información tendiente a requerir o iniciar una investigación. La información proporcionada puede solamente ser utilizado para fines específicos y debe permanecer confidencial.[117] Los pedidos de ayuda pueden también referirse a la preservación expedita de datos guardados en computadoras.[118] Si una tercera Parte estaba involucrada en la transmisión de una comunicación, la Parte puede requerir que se revele una cantidad suficiente de información a fin de identificar al proveedor del servicio y el camino que fue utilizado para la comunicación.[119] Cuando una Parte requiere el acceso, incautación, obtención o revelación de la información guardado en

[117] Proyecto de Convención sobre Delitos Cibernéticos, Artículo 23.
[118] Proyecto de Convención sobre Delitos Cibernéticos, Artículo 24.
[119] Proyecto de Convención sobre Delitos Cibernéticos, Artículo 25.

computadoras, la Parte requerida debe responder tan rápido como sea posible de la siguiente manera:

a) Cuando así lo permita la legislación interna, ratificar o apoyar cualquier autorización judicial o legal que fuera otorgada en la Parte peticionante a fin de efectuar una búsqueda o incautación de la información, ejecutando dicha búsqueda o incautación y, segundo los tratados mutuos de asistencia o las leyes, cuando sean aplicables, procedimiento a revelar a la Parte peticionante cualquier información incautada; o

b) Respondiendo al pedido y revelando la información incautada, segundo lo dispongan sus tratados de asistencia mutua, o las leyes, cuando aplicables; o

c) Utilizando cualquier otro método de ayuda permitido por su legislación interna.

A fin de asegurar la ayuda inmediata en forma de asesoría técnica, la preservación de la información, o la obtención de pruebas, la facilitación de información legal, la localización de los sospechosos, necesita establecerse un punto de contacto disponibles durante las 24 horas los 7 días de la semana.[120]

Mientras que el Proyecto de Convención sobre Delitos Cibernéticos trata de asuntos de ley penal, sus disposiciones sobre asistencia legal mutua pueden no obstante ser de valor para los esfuerzos internacionales destinados a proteger la información personal, particularmente en virtud del hecho de que la Convención trata con un aspecto de la ley que está sumamente relacionado.

c) Los delitos cibernéticos y los Países del G-8

Un proceso paralelo sobre el asunto de los delitos cibernéticos está llevándose a cabo bajo los auspicios de los países del G-8. En la Conferencia Ministerial sobre los Países del G-8 sobre el Combate al Crimen Transnacional Organizado celebrado el 19-20 de octubre de 1999, fue emitida una declaración de los principios sobre acceso transfronterizo a la información almacenada en las computadoras, y que también contiene disposiciones sobre "rápida asistencia mutua":[121]

4. Al recibir un pedido formal para el acceso, búsqueda, copiado, incautación o revelación de datos, incluyendo datos que han sido preservados, el Estado requerido, de acuerdo con su legislación interna, deberá ejecutar el pedido tan rápido como sea posible, de la siguiente manera:

a. Respondiendo según los procedimientos legales y tradicionales de ayuda; o

b. Ratificando o endosando cualquier autorización judicial o legal que fuera otorgada en el estado peticionante y, segundo los procedimientos legales y tradicionales de asistencia, revelando al Estado solicitante cualquier información incautada;

c. Utilizando cualquier otro método de asistencia permitido por la legislación del Estado requerido.

5. Cada Estado, en las circunstancias apropiadas, deberá aceptar y responder a los pedidos de asistencia legal efectuados según estos Principios mediante medios de comunicación rápidos pero confiables, incluyendo la voz, fax o correo electrónico, con confirmación por escrita a seguir cuando sea requerido.

---

120 Proyecto de Convención sobre Delitos Cibernéticos, Artículo 27.

121 "Communique: Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (Moscow, October 19-20,1999)", en-línea: Canada. Department of Foreign Affairs and International Trade, <http://www.dfait-maeci.gc.ca/foreignp/g7/1999/moscow1-e.htm>.b

Nuevamente, existe reconocimiento de que la efectiva ayuda mutua se requiere a fin de tratar cuestiones relacionadas con información almacenada en un Estado extranjero.

IV. CONCLUSIÓN

La protección de la información personal y los datos almacenados de manera electrónica en el sector privado ha avanzado por medio de la adopción de instrumentos internacionales. Los Principios de la OCDE, la Convención del Consejo de Europa, los Lineamientos de las Naciones Unidas, y particularmente la Directiva de Protección de Datos de la UE han tenido un impacto profundo sobre la protección de datos en Europa y en todas partes. También algunos países miembros de la OEA especialmente Canadá y Chile, han promulgado leyes que proporcionan relativamente alto niveles de protección de la privacidad.

Sin embargo, parece justo mencionar que muchos retos permanecen aún, particularmente con relación al flujo transfronterizo de datos personales en la Internet y otras redes globales. La privacidad de los ciudadanos permanece vulnerable aún en aquellos países que cuentan con leyes internas efectivas, en virtud de la existencia de abrigos para la información donde no se encuentra protección disponible. Los instrumentos nacionales e internacionales existentes dejan muchos problemas sin resolver, tales como el de la interpretación sobre qué son los niveles de protección “adecuados” o “equivalentes” o la naturaleza de la observancia requerida a fin de implementar estándares adoptados. La legislación y la observancia son especialmente desafiantes en virtud del rápido desarrollo de la tecnología. Además, aquellos Estados que desean proteger la privacidad de sus ciudadanos deben también enfrentar intereses conflictivos en el área económica, de comercio, social y política.

Estas dificultades, no obstante, no son privativas del área de protección de datos. Se podrían obtener más progresos en el área de la protección a la privacidad mediante una combinación de medidas, incluyendo el desarrollo de estándares internacionales y mecanismos de aplicación, asistencia mutua legal y técnica, el estímulo hacia la autorregulación industrial, y la operación de las fuerzas del mercado influenciadas por la información y la educación.

Sin embargo, debido a la información limitada con que se contaba para efectuar este informe, es difícil evaluar cuán adecuada es la legislación en los países de la OEA. En consecuencia se recomienda que a fin de obtener una evaluación más completa sobre los asuntos jurídicos relacionados con la protección de los datos personales en dichos países, la Subsecretaría de Asuntos Jurídicos reitera este pedido a los Estados miembros, a fin de recabar mayor información sobre la legislación interna vigente, los reglamentos y las políticas adoptadas.