CONSEJO PERMANENTE DE LA
ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

COMISIÓN DE ASUNTOS JURÍDICOS Y POLÍTICOS

OEA/Ser.G
CP/CAJP-3063/12
3 abril 2012
Original: inglés/español

ESTUDIO COMPARATIVO: PROTECCION DE DATOS EN LAS AMÉRICAS

Diversos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, incluidas leyes, reglamentos y autoregulación nacionales

[Documento presentado por el Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos, conforme al párrafo operativo 10 de la resolución AG/RES. 2661 (XLI-O/11)

ESTUDIO COMPARATIVO: PROTECCION DE DATOS EN LAS AMÉRICAS

Diversos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, incluidas leyes, reglamentos y autoregulación nacionales

-- Índice de contenido --

ESTUDIO COMPARATIVO: PROTECCION DE DATOS EN LAS AMÉRICAS

Diversos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, incluidas leyes, reglamentos y autoregulación nacionales

[Documento presentado por el Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos, conforme al párrafo operativo 10 de la resolución AG/RES. 2661 (XLI-O/11)]

I. Introducción

Desde hace mucho tiempo, la Asamblea General de la Organización de los Estados Americanos ha prestado especial atención a los asuntos relacionados con el acceso a la información y la privacidad/protección de datos. Como prueba de ello, en la cuarta sesión plenaria de la Asamblea General, celebrada el 7 de junio de 2011, se aprobó la resolución AG/RES. 2661 (XLI-O/11) en la que se encomendó al Departamento de Derecho Internacional la realización del presente estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, incluso las leyes, reglamentos y autoregulación nacionales (el "estudio comparativo"), con miras a explorar la posibilidad de un marco regional en esta área[1/].

Dando seguimiento a la resolución antes indicada, la Comisión de Asuntos Jurídicos y Políticos (CAJP), en su sesión ordinaria del 6 de octubre de 2011, estableció un calendario y un proyecto de metodología, así como el proceso mediante el cual los Estados Miembros de la Organización harían sus comentarios sobre los marcos jurídicos existentes en materia de privacidad/protección de datos, necesarios para este estudio. En dicha sesión, las delegaciones solicitaron la elaboración de un cuestionario sobre legislación y prácticas en materia de privacidad y protección de datos, de tal manera que los Estados Miembros pudieran ofrecer la información solicitada en un formato estándar. Dicho cuestionario fue elaborado y distribuido el 31 de octubre de 2011 como documento CP/CAJP-3026/11. El plazo para la entrega de respuestas a la Presidencia de la CAJP fue fijado para el 15 de enero de 2012, aunque fue prorrogado hasta el 15 de febrero del mismo año. Asimismo, los Estados Miembros convinieron en que las aportaciones de otros órganos, organismos y entidades del sistema interamericano serían incorporadas en el estudio (incluido el estudio sobre acceso a la información y protección de datos contenido en el documento CP/doc.

1. AG/RES. 2661 (XLI-O/11), aprobada el 7 de junio de 2011. Como preámbulo a este mandato, la Asamblea General recordó que el acceso a la información pública, por un lado, y la protección de datos personales, por el otro, son valores fundamentales que deben trabajar siempre en concordancia; consideró la creciente importancia de la privacidad y la protección de datos personales, así como la necesidad de fomentar y proteger el flujo transfronterizo de información en las Américas; tuvo presentes los esfuerzos de los Estados para garantizar el acceso a la información pública y la protección de datos personales, así como los esfuerzos de otras entidades internacionales y regionales tales como la Organización de Cooperación y Desarrollo Económicos (OCDE), el Foro de Cooperación Económica Asia-Pacífico (APEC), la Unión Europea y el Consejo de Europa, que trabajan en el área de la protección de datos personales; y tomó nota del Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos Personales (CP/CAJP-2921/10 rev. 1), preparado por el Departamento de Derecho Internacional, así como los comentarios de los Estados Miembros al mismo.

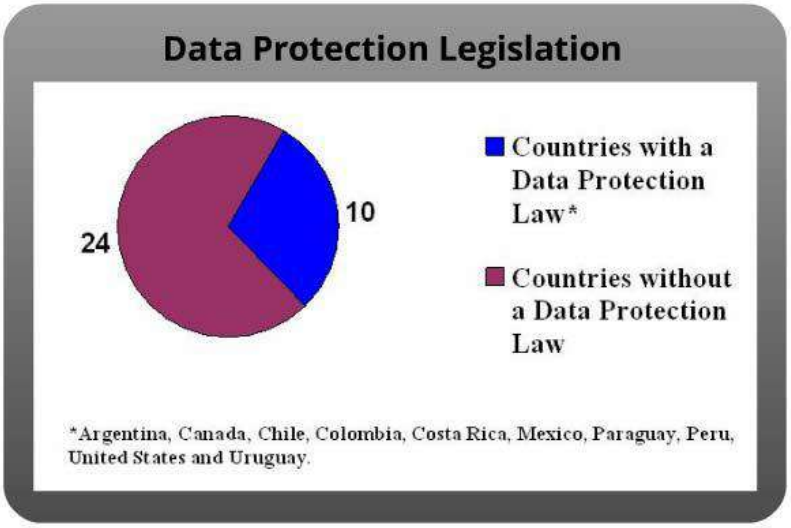
4193/07), así como las aportaciones de otras organizaciones internacionales que trabajan en el área de la privacidad/protección de datos.

Los siguientes Estados Miembros respondieron el cuestionario: Argentina, Canadá, Colombia, Costa Rica, El Salvador, Estados Unidos, México, Panamá, Perú, República Dominicana y Uruguay. La información recopilada de esta forma ha quedado plasmada en la primera parte de este estudio. Asimismo, se incluye un breve resumen de la labor que realizan otras organizaciones internacionales, incluido el APEC, el Consejo de Europa, la Unión Europea, la Red Iberoamericana de Protección de Datos (RIPD) y la OCDE.

En la sección II del estudio se hace una comparación general de los marcos jurídicos existentes en materia de privacidad/protección de datos. En la sección III se ofrecen breves resúmenes de los instrumentos internacionales adoptados o de las labores que realizan otras organizaciones internacionales en materia de privacidad/protección de datos. En la sección IV se ofrece una descripción de los marcos jurídicos locales en materia de privacidad/protección de datos de los Estados Miembros de la OEA.

II. Marcos jurídicos generales

La legislación sobre la protección de datos se basa en el derecho de las personas a la privacidad. Sin embargo, pueden variar el significado de privacidad y el origen del derecho a la privacidad de una persona. Por esa razón, las leyes y políticas que rigen este derecho difieren de un país a otro. Habida cuenta de esta divergencia en el tratamiento del derecho a la privacidad, la legislación que protege el tratamiento de los datos personales puede variar de una región a otra e incluso dentro de una misma región. En términos generales, el tratamiento de la protección de datos ha seguido uno de tres criterios. El europeo es hoy el sistema más estricto de regulaciones estatales, con una legislación que rige la recolección de datos personales por parte del Gobierno y las entidades privadas. El sistema de Estados Unidos sigue un criterio bifurcado, que permite que los sectores económicos regulen los datos personales recabados por organizaciones privadas y la regulación estatal de los datos recabados por el Estado. Por último, varios países de América Latina tienen mecanismos de protección de datos basados en el concepto de habeas data, el cual es un derecho constitucional que permite a las personas acceder a sus propios datos personales y otorga el derecho a corregir toda información errónea. Asimismo, varios países latinoamericanos han adoptado recientemente leyes exhaustivas sobre la privacidad/protección de datos.



La Declaración Universal de Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos definen a la privacidad como un derecho a no ser "objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a" la "honra y reputación" de la persona. Los dos tratados explican luego que "[t]oda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". El Consejo de Europa reconoce también el derecho a la privacidad como un "derecho humano fundamental".

En la mayoría de los países, los orígenes del concepto de privacidad pueden encontrarse en sus constituciones políticas. Por ejemplo, en Estados Unidos y Canadá este concepto se deriva en gran parte de los preceptos constitucionales contra un registro e incautación irracionales. En sus decisiones, la Suprema Corte ha declarado que la Constitución protege "el derecho de las personas de evitar la divulgación de sus asuntos personales" y "el derecho a la independencia para tomar cierto tipo de decisiones importantes"[2/]. Sin embargo, la Suprema Corte también ha sostenido que el derecho a la privacidad no es absoluto y que el interés de una persona por su privacidad debe ponderarse frente a la competencia del interés público[3/].

En Latinoamérica, los marcos constitucionales de varios países definen la privacidad como el derecho a que la intimidad de una persona, su familia, su hogar o su correspondencia no sean objeto de interferencias arbitrarias y el derecho a que su honor y su reputación estén libres de ataques, según se define en la Declaración Universal de Derechos Humanos y en el Pacto de Derechos Civiles y Políticos. En algunas constituciones se incluye el derecho a la protección de datos y algunas disposiciones sobre el recurso de habeas data.

---

2. En Estados Unidos, el derecho a la privacidad suele definirse como "el derecho no ser molestado". La Suprema Corte ha fallado en favor de la privacidad acogiéndose a lo estipulado en la Cuarta Enmienda de la Constitución.
3. Íd.

Constitutional Provisions which expressly provide for a right to Privacy, Habeas Data and/or Data Protection

Country	Privacy	Habeas Data	Data Protection
Argentina	Yes art. 18	Yes art. 43	No
Brazil	Yes art. 5	Yes art. 5	No
Canada	Yes section 7 & 8	No	No
Chile	Yes art. 19	No	No
Colombia	Yes art. 15	Yes art. 15	No
Costa Rica	Yes art. 24	No	No
Dominic Republic	Yes art. 44	Yes art. 70	Yes art. 44
Ecuador	Yes art 66	Yes art. 94	Yes art. 66
El Salvador	Yes art. 2	No	No
Guatemala	Yes art. 25	Yes art. 31	No
Mexico	Yes art. 6	Yes art. 16	Yes art. 16
Panama	Yes art. 29, 17, 37	Yes art. 44	No
Paraguay	Yes art. 30	Yes art. 135	No
Peru	Yes art. 2	Yes art. 200	Yes art. 2
United States	Yes 4th amendment	No	No
Uruguay	Yes art. 7	No	No
Venezuela	Yes art. 60	Yes art. 281	Yes art. 28

III. Instrumentos internacionales sobre privacidad/protección de datos

Diversas organizaciones multilaterales han realizado grandes esfuerzos en las últimas décadas para adoptar directrices, principios, recomendaciones o instrumentos jurídicos vinculantes, en los ámbitos regional e internacional, en particular la OCDE, el Consejo de Europa, la Unión Europea y el APEC. Existen algunos elementos comunes en estos instrumentos que se aplican y que tienen un impacto diverso en los marcos jurídicos de los Estados Miembros de la OEA. En términos generales, indican que la información personal debe ser obtenida de manera justa y lícita, que se utilice en formas que sean compatibles con el propósito original especificado, que sea precisa, pertinente y proporcional con respecto a este propósito, que sea verídica y actualizada, que no se distribuya fácilmente a terceros y que se destruya una vez que se cumpla su propósito. Al mismo tiempo, existen algunas diferencias significativas en el planteamiento de estos instrumentos, incluso cómo y cuándo deben aplicarse los mismos principios a entidades gubernamentales, a proveedores de servicios públicos, a empresas privadas y a personas, la aplicación del derecho penal y la seguridad nacional[4/].

A. APEC

Durante varios años el Foro de Cooperación Económica Asia-Pacífico (APEC) ha estado trabajando en una iniciativa sobre privacidad. Sin embargo, más que buscar la armonización de leyes internas sobre privacidad, el APEC se ha enfocado específicamente en el tema de las transferencias

4. Comentarios preliminares sobre una declaración de principios para la protección de la privacidad y de los datos personales en las Américas, CJI/doc.382/11.

de datos personales entre países. En 2004 se adoptó un Marco con Principios sobre Privacidad, al que se agregó un programa de implementación en 2005, a fin de fomentar la implementación de los Principios entre los Estados Miembros. Un subgrupo sobre Privacidad de Datos ha estado trabajando para desarrollar reglas de privacidad transfronterizas, con las que se autorizaría a las empresas a transferir información personal entre los países que participan en el APEC. Además, en 2010 se estableció un Acuerdo de Cooperación para la Observancia de la Privacidad Transfronteriza (conocido por su sigla en inglés como CPEA) con el fin de brindar reconocimiento mutuo entre las economías que participan en el APEC sobre los mecanismos de cada parte para la certificación de las reglas de privacidad de los negocios. (La OCDE posee una red similar de aplicación llamada GPEN (Red Global de Protección de la Privacidad.)

B. Consejo de Europa

El Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal define en términos generales los datos personales como "toda información relacionada con una persona identificada o identificable" y describe los principios de la protección de datos, que han servido de base para la legislación en este campo en todo el mundo. [5/] Este convenio consiste en tres partes principales: preceptos sustantivos en forma de principios básicos, reglas específicas sobre los flujos transfronterizos de datos y los mecanismos de asistencia mutua y consulta entre las partes.

El punto de partida de este convenio es que pueden ser protegidos algunos derechos de la persona con respecto al libre flujo de la información entre fronteras.[6/] Cuando este convenio impone algunas restricciones o condiciones al ejercicio de la libertad de información, lo hace solo en la medida de lo estrictamente justificado para la protección de los derechos y libertades de la persona, en particular el derecho al respeto de la privacidad.[7/]

En la actualidad el Convenio 108 está siendo revisado con dos objetivos principales: hacer frente a los retos a la privacidad resultantes del uso de nuevas tecnologías de la información y fortalecer los mecanismos de seguimiento del convenio.

C. Unión Europea

En la Directiva sobre Protección de Datos de la Unión Europea se reconoce el derecho de la persona a la privacidad y se fija el nivel estándar de la protección de datos para los miembros de la Unión Europea.[8/] A raíz de esta preocupación expansiva por el derecho a la privacidad del individuo, la Directiva pasa a admitir la transferencia de datos personales a países de fuera de la Unión Europea

---

5. *Véase* Consejo de Europa, Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, arts. 2, 4-12, 28 de enero de 1981.
6. Nota explicativa al Convenio 108. Este principio está consagrado en los instrumentos internacionales y europeos sobre derechos humanos. *Véase* el artículo 10 del Convenio Europeo de Derechos Humanos; artículo 19 del Pacto Internacional de Derechos Civiles y Políticos.
7. Artículo 8, Convenio Europeo de Derechos Humanos.
8. *Véase* Stratford, pág. 19 (donde se agrega que la *Directiva*, que fue aprobada en 1995, encomendaba a los Estados miembros asegurar que su legislación nacional sobre privacidad cumpliera con sus normas).

solo cuando el país afectado "garantice un nivel de protección adecuado [de los datos]" o si demuestra que los datos quedarán debidamente protegidos una vez que hayan sido transferidos.[9/] De esta manera, la Directiva amplía a los países fuera de sus fronteras el alcance de la protección otorgada a los datos personales originados en la Unión Europea.

El alcance de la Directiva se ha extendido más allá de las fronteras europeas y ha incidido en la regulación de la protección de datos en todo el mundo, al obligar a otros países con empresas interesadas en transferir datos personales a examinar su propia legislación sobre protección de datos y, de ser necesario, modificarla para satisfacer los estándares de la Unión Europea.[10/] Cabe destacar, sin embargo, que la Comisión Europea emprendió una revisión de la Directiva en 2010 debido, en parte, a que "es preciso mejorar, en general, los mecanismos existentes de transferencia internacional de datos personales". El Vicepresidente de la Comisión Europea responsable de la Agenda Digital ha explicado también que el marco regulatorio relativo a la protección de datos de la Unión Europea debe ser actualizado conforme a la era digital a fin de proteger los derechos fundamentales y, al mismo tiempo, "tener la mejor economía y mejores condiciones de vida que permiten las tecnologías digitales". Se anticipa que hacia finales de año se presente una propuesta para una nueva ley que reemplace a la Directiva.

D. Organización de Cooperación y Desarrollo Económicos

La Organización de Cooperación y Desarrollo Económicos (OCDE) adoptó una serie de principios no vinculantes y neutros desde el punto de vista tecnológico que podrían utilizarse para establecer un marco jurídico o una norma industrial. Las ocho Directrices que Rigen la Protección de la Privacidad y de los Flujos Transfronterizos de Datos Personales se aplican para los usos de datos personales tanto en el ámbito gubernamental como en el privado.[11/] Establecen: 1) limitar la captura de datos personales y asegurar que dicha información pueda solamente obtenerse por medios legítimos y justos y, cuando sea apropiado, mediando el conocimiento o el consentimiento del titular de los datos; 2) asegurar que la información recopilada sea pertinente para los fines para los cuales será utilizada, debiendo también ser precisa, íntegra y actualizada; 3) especificar las finalidades para las cuales se recopilan los datos personales; 4) no divulgación ni uso de los datos para fines diferentes de aquellos especificados con anterioridad; 5) proteger los datos mediante salvaguardias que otorguen razonable seguridad; 6) establecer una política general de apertura sobre avances, prácticas y políticas relacionadas con los datos personales; 7) brindar a los individuos el derecho de obtener datos personales dentro de un plazo razonable y también de manera razonable, y 8) responsabilizar a los controladores de datos por el cumplimiento de los requerimientos contenidos en estos principios.

La OCDE anotó también una Recomendación Relativa a la Cooperación Transfronteriza en la Aplicación de las Legislaciones que Protegen la Privacidad.[12/] Entre otras cosas, en este

---

9 . Íd.

10. Íd. págs. 19 y 20.

11. Directrices que Rigen la Protección de la Privacidad y de los Flujos Transfronterizos de Datos Personales, adoptados en 1980, disponibles en: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

12. Recomendación Relativa a la Cooperación Transfronteriza en la Aplicación de las Legislaciones que Protegen la Privacidad, adoptada en 2007, disponible en: http://www.oecd.org/document/60/0,3343,en_2649_34255_38771516_1_1_1_1,00.html.

documento se sugiere el establecimiento de una red informal de autoridades encargadas de la aplicación de leyes en materia de privacidad.[13/] La red GPEN es un esfuerzo de la OECD –similar al acuerdo CPEA del APEC– para poner en práctica esta recomendación.[14/]

IV. Marcos jurídicos nacionales

La exposición sobre privacidad/protección de datos en los Estados Miembros se divide en cuatro secciones: en la sección A se describe, según la información disponible, si en la constitución de un Estado se establece un derecho a la privacidad, un derecho a la protección de datos o el recurso del habeas data; se analiza si el Estado ha promulgado leyes (de amplio alcance, sectoriales o basadas en principios) en materia de privacidad/protección de datos o legislaciones sobre el recurso de habeas data; se expone si estas leyes se aplican a contextos del sector privado o público, y si el marco local dispone de códigos de conducta autorregulatorios o sistemas el similares de rendición de cuentas en materia de privacidad/protección de datos.[15/]

En la sección B se analiza, según la información disponible, si el sistema local establece o dispone la creación de una entidad encargada de la protección/aplicación de leyes en materia de datos y describe su relación con (o independencia de) el Gobierno; analiza la forma en que cada Estado hace cumplir las leyes, reglamentos y procesos en materia de privacidad/protección de datos, y se exponen los recursos disponibles en caso de violación y describe también los medios de que disponen las personas afectadas por una violación. Cuando se dispone de información, se expone el volumen y tipo de quejas atendidas por o presentadas ante las autoridades, y si tales autoridades tienen las capacidades para llevar a cabo una investigación y si quienes cometen tales violaciones pueden ser sujetos de sanciones penales.

En la sección C se describe, según la información disponible, el sistema de que dispone cada Estado para la cooperación transfronteriza; se describe si el Estado establece límites o condiciones a la transferencia de datos personales a otros países; se analizan los marcos para los flujos transfronterizos de información [si datos personales que se refieren a un residente del Estado o datos que fueron procesados en el Estado pueden ser transferidos (exportados o compartidos con) otra jurisdicción]; se describe el sistema de cooperación transfronteriza cuando ocurre una violación o una contravención en el ámbito local con respecto a datos que se originan en una jurisdicción extranjera, o cuando ocurre una violación o contravención en una jurisdicción extranjera sobre datos personales locales, y se describen los acuerdos internacionales o de los que sea parte el Estado, incluso si cuenta con la certificación en materia de privacidad/protección de datos de la Unión Europea. En caso de que se disponga de la información, en esta sección se intentará analizar si las leyes locales

---

13. En el párrafo 21 de la Recomendación Relativa a la Cooperación Transfronteriza en la Aplicación de las Legislaciones que Protegen la Privacidad se detalla una serie de tareas para la red: debatir los aspectos prácticos de la cooperación en la aplicación de las leyes en materia de privacidad; intercambio de prácticas óptimas en el tratamiento de retos transfronterizos; establecimiento de prioridades compartidas en materia de aplicación de leyes, y apoyo a las iniciativas conjuntas y aplicación de leyes y campañas de concienciación.
14. El sitio web de la red GPEN se encuentra en: https://www.privacyenforcement.net.
15. A no ser que se agregue una fuente o cita especifica como nota de pie página, la información contenida en esta sección se refiere específicamente a las respuestas al Cuestionario de Legislación y Prácticas sobre Privacidad y Protección de Datos presentado por el Estado en cuestión.

permitieron a las autoridades compartir información sobre sus métodos de investigación y aplicación con autoridades en otras jurisdicciones, incluso si tal colaboración es informal o si se lleva a cabo a través de reguladores o redes de cooperación transfronterizas, por ejemplo, la red GPEN, el acuerdo CPEA del APEC o la RIPD.

En la sección D se examina el efecto de la jurisprudencia pertinente sobre la privacidad/marco de protección de datos, así como cualquier reto especial que enfrente el Estado en cuestión.

1. Argentina

A. Contexto jurídico

i. Marco constitucional

Un análisis de los derechos constitucionales en materia de privacidad/protección de datos en Argentina[16/] inicia con una exposición sobre los instrumentos internacionales pertinentes relativos a la libertad de expresión e información, incluida la Declaración Americana de los Derechos y Deberes del Hombre, la Declaración Universal de los Derechos Humanos[17/], la Convención Americana sobre Derechos Humanos[18/], el Pacto Internacional de Derechos Económicos, Sociales y Culturales, así como el Pacto Internacional de Derechos Civiles y Políticos y su Protocolo Facultativo.[19/] Estos

16. Constitución, arts. 14, 33 y 32.
17. Artículo 19: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."
18. Artículo 13. Libertad de pensamiento y de expresión 1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas. 3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.
19. Artículo 19: 1. Nadie podrá ser molestado a causa de sus opiniones. 2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.

instrumentos tienen jerarquía constitucional en Argentina[20/] y los derechos consagrados en cada uno de ellos también han sido expresamente incluidos en la Constitución del país.[21/]

Por lo que se refiere a la privacidad/protección de datos, en el artículo 43 de la Constitución se establece el derecho de habeas data, según el cual cualquier persona puede interponer una acción para tomar conocimiento de los datos a ella referidos y, en caso de falsedad o discriminación, para solicitar la supresión, rectificación, confidencialidad o actualización de dichos datos. [22/]

En el artículo 19 se reconoce el derecho constitucional a la privacidad, disponiendo en parte que las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios y exentas de la autoridad de los magistrados. En el artículo 18 se establece que la correspondencia y los documentos privados están protegidos expresamente, disponiendo en parte que la correspondencia escrita y los documentos privados son inviolables.

---

20. En el apartado 22 del artículo 75 se establecen los tratados y acuerdos que tienen jerarquía superior a las leyes nacionales.
21. Artículo 14: Todos los habitantes de la Nación gozan de los siguientes derechos conforme a las leyes que reglamenten su ejercicio, a saber: de trabajar y ejercer toda industria lícita; de navegar y comerciar; de peticionar a las autoridades; de entrar, permanecer, transitar y salir del territorio argentino; de publicar sus ideas por la prensa sin censura previa; de usar y disponer de su propiedad; de asociarse con fines útiles; de profesar libremente su culto; de enseñar y aprender. Artículo 32: El Congreso federal no dictara leyes que restrinjan la libertad de imprenta o establezcan sobre ella la jurisdicción federal. Artículo 33: Las declaraciones, derechos y garantías que enumera la Constitución no serán entendidos como negación de otros derechos y garantías no enumerados; pero que nacen del principio de la soberanía del pueblo y de la forma republicana de gobierno.
22. Artículo 43.

ii. Marco legislativo

La Ley Federal de Protección de los Datos Personales[23/], y su reglamentación[24/], tiene aplicabilidad en todo el país, y su objetivo es la protección de los datos personales procesados por medios tecnológicos. Esta ley se aplica a todas las bases de datos públicas (sin límite alguno), así como a todas las bases de datos privadas que no sean para uso personal.

La ley define y protege los datos de naturaleza delicada, establece los principios y requisitos de calidad y procesamiento de los datos, regula actividades de transferencia, la transferencia internacional, la prestación de servicios, los informes de crédito y actividades de mercadotecnia, prescribe la obligación de registrar las bases de datos, las medidas de seguridad y confidencialidad, el derecho de la persona (propietario de los datos) a tener acceso a ellos, rectificarlos, corregirlos y suprimirlos, crea la autoridad encargada de la protección de datos y dispone las sanciones administrativas.[25/]

23. Ley N.º 25.326.
24. Decreto N.º 1.558/2001
25. Ley N.º 25.326 de Protección de Datos Personales y su reglamentación, Decreto N.º 1.558/2001, (DNPDP Disposición N.º 11/06).

iii. Habeas data

La ley N.º 25.326 de Protección de Datos Personales y su reglamentación, Decreto No. 1.558 /2001, regula también la acción judicial del habeas data.

iv. Autoregulación

La Ley de Protección de Datos permite la creación voluntaria de "códigos de conducta" mediante los cuales las asociaciones privadas, organizaciones o usuarios de los datos pueden elaborar sus códigos deontológicos, en los que se establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley. Dichos códigos deberán ser inscritos en el registro que al efecto lleve el organismo de control. Este organismo podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.[26/]

Hasta la fecha, solo ha quedado registrado un código de conducta ante la Dirección Nacional de Protección de Datos Personales (DNPDP), según la solicitud presentada por la Asociación de Marketing Directo, aprobada en 2004 conforme a lo dispuesto por la ley.[27/]

B. Ejecución

i. Mecanismo de ejecución

Básicamente, existen dos mecanismos de ejecución del derecho a la privacidad/protección de datos, a saber: a) el mecanismo administrativo a través de la DNPDP, y b) el poder judicial a través del recurso de habeas data o alguna acción de carácter ordinario.

En el ámbito administrativo, la DNPDP recibe quejas o actúa por su cuenta ante posibles violaciones de la ley.[28/] El artículo 31 del Decreto correspondiente a la Ley N.º 25.326 se aplica a bases de datos públicas y privadas. Por regla general, el procedimiento administrativo incluye los pasos enumerados más adelante, iniciados por la DNPDP, en los casos de supuestas violaciones de las disposiciones de la Ley N.º 25.326 y su reglamentación. La DNPD puede actuar ex oficio o al recibir una queja de una persona, de la Oficina del *Ombudsman*, o de un grupo de consumidores usuarios. Seguidamente, la DNPDP abrirá un expediente en el cual se habrán de registrar los hechos particulares del caso y la verificación de la supuesta infracción. La supuesta parte infractora tendrá cinco días hábiles para presentar su defensa por escrito y proporcionar cualquier prueba de que no han ocurrido las violaciones. Luego de que en la DNPDP emita su fallo puede presentarse una apelación en un plazo de 10 días hábiles.

En el ámbito judicial, la persona puede interponer una acción conforme a lo dispuesto en el artículo 43 de la Constitución, referente al recurso de habeas data, y la ley de protección de datos: a)

---

26. Ley N.º 25.326, artículo 30 y Decreto 1558/2001.
27. Resolución DNPDP N.º 4/2004.
28. Ley N.º 25.326, artículo 31 y Decreto 1558/2001.

para tomar conocimiento de datos personales que consten en registros o bancos de datos públicos o privados y b) en caso de que los datos sean incorrectos, falsos, imprecisos, anticuados, etc. o cuando su procesamiento esté prohibido por la ley, para exigir su rectificación, supresión o actualización.[29/]

ii. Protección de datos/autoridades ejecutoras

La autoridad en la materia en Argentina es la DNPDP[30/], que forma parte de la estructura del Ministerio de Justicia y Derechos Humanos, aunque tiene independencia en el cumplimiento de sus deberes.[31/] Está conformada por aproximadamente 45 personas y su presupuesto depende del Ministerio de Justicia y Derechos Humanos.

La DNPDP está obligada a atender todas las quejas que supongan una violación de la ley. Como entidad supervisora, autorizada para recibir quejas, la DNPDP ha recibido un promedio de 500 quejas al año, cifra que ha estado disminuyendo a medida que se conoce más acerca del marco legal sobre la privacidad/protección de datos.

La mayoría de las quejas contra entidades privadas se refieren a violaciones a los derechos de acceso, rectificación, supresión, etc., en tanto que aquellas contra entidades del sector público están vinculadas con violaciones al derecho de acceso a datos personales.

Por lo que se refiere al volumen de quejas contra entidades privadas, aproximadamente el 70 % son contra instituciones financieras, 10 % contra compañías de calificación de crédito y 20 % contra empresas de servicios públicos y otras. De las quejas procesadas, el 80% de las veces se falló en favor de la parte actora (acceso, rectificación, supresión, bloqueo, etc.). En aproximadamente 14 % de los casos se determinó que no se había violado el reglamento existente; y el 2 % de las quejas fue suspendido porque ya existía un proceso paralelo en el sistema judicial. En otro 2 % de los casos, la DNPDP se declaró incompetente para atender la queja y el último 2 % no fue posible procesarlas debido a fallas de procedimiento.

iii. Sanciones administrativas y penales

La ley establece sanciones administrativas para las bases de datos públicas por responsabilidad legal o por daños resultantes de la observancia de la ley pertinente.[32/] La DNPDP puede emitir una advertencia, suspensión, multas, u ordenar el cierre o cancelación del archivo, registro o base de datos.[33/] En la reglamentación se definen las condiciones y procedimientos para la aplicación de las sanciones, graduadas según su gravedad y magnitud de la violación y daños provocados. El artículo 31 del Decreto correspondiente a la Ley N.º 25.326 se aplica a bases de datos públicas y privadas. Según se ha indicado, las sanciones son graduadas según la gravedad del caso, para lo cual se toma en cuenta la naturaleza de los derechos personales afectados, el volumen de las operaciones procesadas, los beneficios obtenidos, el grado de intencionalidad, la reincidencia, los daños causados a las personas afectadas y terceros, y cualquier otra circunstancia pertinente para

29. Ley N.º 25.326, capítulo VII.
30. Ley N.º 25.326, art. 29.
31. Decreto N.º 1558/01, art. 29.
32. Ley N.º 25.326, art. 31. Asimismo, pueden aplicarse sanciones penales según se indica en la sección IV de este documento.
33. Según la ley, las multas pueden variar desde US$1 000 hasta US$100.000.

determinar la ilegalidad y culpabilidad específicas. Aquellas personas declaradas culpables de una violación a la Ley N.º 25.326 y su decreto y que reincidan en un período de tres años serán objeto también de sanciones más severas.[34/]

El Código Penal de Argentina dispone también sanciones penales en materia de protección de datos.[35/] En términos generales, las personas que a sabiendas inserten información falsa en una base de datos pueden recibir pena desde un mes hasta dos años de cárcel. Las personas que a sabiendas proporcionen información falsa a un tercero podrán recibir pena desde seis meses hasta tres años de cárcel, aunque ésta puede aumentar 1,5 veces el mínimo o máximo cuando las personas sufran daños como resultado de tales acciones conscientes y deliberadas. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, quedará inhabilitado para el desempeño de cargos públicos por el doble del tiempo de la condena. En el Código Penal se estipula un artículo adicional con el que se castiga con pena de cárcel desde un mes hasta dos años a cualquier persona que de manera consciente e ilícita viole los sistemas de seguridad y confidencialidad de datos, o que tenga acceso ilícito a datos personales, o que divulgue información contenida en bases de datos personales, que debería ser confidencial según lo dispuesto por la ley. Cuando el autor del delito sea un funcionario público, quedará inhabilitado por un período de uno a cuatro años.[36/]

C. Cooperación transfronteriza

i. Transferencia de datos

La legislación argentina prohíbe la transferencia de datos personales a países que no cuentan con leyes que ofrezcan protecciones similares a las estipuladas en la Ley N.º 25.326. Sin embargo, es posible conseguir una excepción, por ejemplo, cuando la persona da su consentimiento para la transferencia o cuando la entidad que importa los datos está obligada por contrato a aplicar la Ley N.º 25.325, siempre y cuando la legislación local no prohíba la aplicación de la ley argentina.[37/]

ii. Instrumentos/acuerdos internacionales

Argentina no es parte de ningún instrumento o acuerdo internacional relativo a los principios generales de privacidad y el flujo transfronterizo de información. Sin embargo, Argentina ha

---

34. El producto de las multas estipuladas en el artículo 31 de la Ley N.º 25.326 se aplicará al financiamiento de la DNPDP.
35. El artículo 32 de la Ley N.º 25.326 se incluye como referencia y posteriormente como estatuto en el artículo 117 bis del Código Penal.
36. El artículo 32 de la Ley N.º 25.326 se incluye como referencia y posteriormente como estatuto en el artículo 157 bis del Código Penal.
37. Ley N.º 25.326, art. 12. La prohibición para la transferencia internacional de datos no regirá en los siguientes casos: a) colaboración judicial internacional; b) intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior; c) transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; d) cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; e) 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.

recibido el certificado de suficiencia como país con una legislación compatible, por decisión de la Comisión Europea[38/] y participa activamente en la RIPD.

iii. Cooperación transfronteriza en materia de investigación y ejecución de las leyes

En Argentina, la cooperación transfronteriza se da generalmente entre los órganos jurisdiccionales o administrativos del Estado de manera informal y recíproca. La ley, sin embargo, no prevé una excepción a la prohibición general contra la transferencia internacional para los casos de colaboración judicial internacional, lo que hace posible y más efectiva la cooperación transfronteriza.[39/]

Además, por razones de jurisdicción territorial, en caso de que se detecten violaciones, las autoridades de locales en materia de protección de datos pueden remitir estos casos a otras autoridades en el país o en el extranjero. Este tipo de cooperación se ha presentado en procesos administrativos, por ejemplo, emanados de quejas en las que se han visto involucrados España y el Reino Unido. En el ámbito local, la cooperación se da entre las oficinas de protección al consumidor que existen en cada provincia, las cuales remiten todos los casos que entran en su jurisdicción a los órganos supervisores.

D. Jurisprudencia y retos especiales

La jurisprudencia en Argentina en materia de privacidad/protección de datos es amplia y ha sido decisiva en el desarrollo de este derecho, así como en la implementación de la legislación. Entre los casos más notables se incluye "Ponzetti de Balbin", "Ganora" y "Urteaga". El caso más reciente y que trascendió a todo el país fue el de "Prudential".[40/]

Por lo que se refiere a los efectos especiales comunes en Argentina, la Internet presenta desafíos particularmente significativos en cuanto a las políticas de privacidad que rigen la operación de los servicios de información empresarial, que deben adaptarse a la protección de la privacidad/datos personales, con especial énfasis en la aplicabilidad del derecho a ser olvidado (por ejemplo, los datos disponibles en línea que permanecen a perpetuidad en la Internet y que interfieren con los derechos de los individuos aunque no tengan valor como novedad). Estos datos suelen convertirse en archivos históricos de información que sigue siendo recuperada por motores de búsqueda tales como Google, Bing, etc.

De igual modo, las tecnologías de verificación y ubicación de contenido (celulares, GPS, RFID, satélite, inalámbrico, radar, antenas, *cookies*, etc.) generan instantáneamente información sobre la ubicación y actividades de las personas, lo cual requiere ser reglamentado. Otras tecnologías son motivo de incomodidad para los usuarios y requieren su propia reglamentación (mercadeo por correo directo o por teléfono, mensajes de texto a teléfonos celulares, etc.).

---

38. *Véase* la respuesta de Argentina al cuestionario en donde se encontrará una copia del certificado de la Unión Europea.
39. Ley N.º 25.326, art. 12 (a).
40. Se adjuntan los casos a la documentación suministrada por Argentina como parte de su respuesta al cuestionario.

2. Canadá

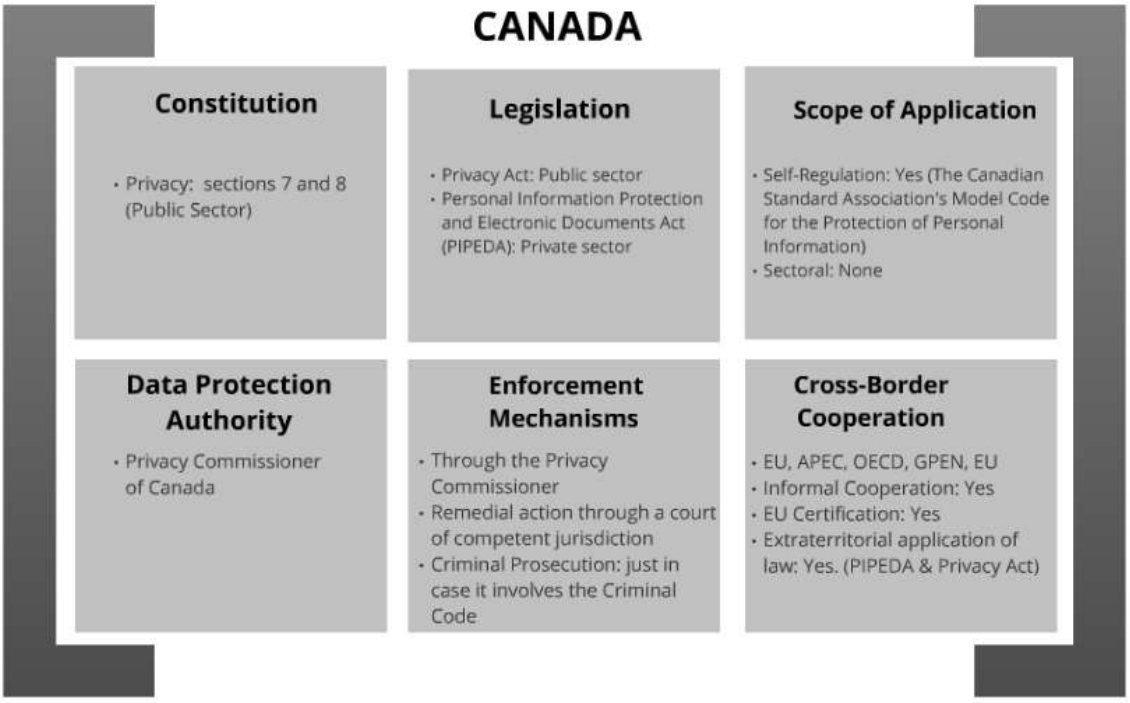
A. Contexto jurídico

i. Marco constitucional

La Carta Canadiense de Derechos y Libertades (la Carta) forma parte de la Constitución de Canadá y se aplica en todos los ámbitos de Gobierno: federal, provincial, territorial y municipal.[41/] Toda acción y decisión del Gobierno se sujeta a la Carta. Algunas acciones de entidades no gubernamentales pueden también quedar sujetas a la Carta cuando tales acciones equivalgan en esencia a "acciones de Gobierno", lo cual se determina de acuerdo con los criterios jurisprudenciales establecidos.

En su sección 8, la Carta establece que cualquier persona "tiene derecho a oponerse a un registro e incautación irracional", lo cual constituye la principal disposición constitucional en materia de recopilación, uso y divulgación de información personal por parte de las instituciones y entidades de Gobierno. Los tribunales canadienses han interpretado esta sección de manera amplia y dependiendo del contexto. Esta sección garantiza que cualquier persona puede esperar razonablemente que su privacidad quede protegida contra cualquier forma de interferencia injustificada por parte del Estado. Cualquier intromisión puede ser considerada como "razonable" –es decir, que cumpla con la sección 8– si ha sido autorizada por la ley. La ley en sí misma debe ser razonable y el registro o incautación debe llevarse a cabo de manera razonable. De tal manera que si cualquier intrusión no está debida y razonablemente autorizada por la ley, cualquier persona que considere que su privacidad ha sido ultrajada –ya sea en su persona, en su hogar o en su información personal que sea divulgada– puede entablar un recurso constitucional, e incluso solicitar resarcimiento.

41. http://laws-lois.justice.gc.ca/eng/charter/



En la sección 7 de la Carta quedan protegidos los derechos a la vida, la libertad y la seguridad de la persona conforme a los principios de justicia fundamental. En ocasiones se ha llegado a considerar que dispone también la protección de la privacidad, incluso la protección de datos.

Si bien la privacidad de los datos queda recogida en la sección 8 de la Carta, podría considerarse que la sección 2(b) desempeña un papel auxiliar en cuanto a la protección de datos en general. La sección 2(b) protege la libertad de expresión en Canadá, y lee textualmente: "Toda persona goza de las siguientes libertades fundamentales: (...) b) libertad de pensamiento, creencias, opinión y expresión, incluso la libertad de expresarse por medios impresos u otros medios de comunicación;..." Los tribunales canadienses han sido muy generosos en su interpretación de esta sección, al grado de exigir que cualquier restricción que imponga el Estado debe satisfacer plenamente lo especificado en la sección 1 de la Carta, que dice textualmente "La Carta Canadiense de Derechos y Libertades garantiza los derechos y libertades en ella estipulados salvo solamente los límites razonables prescritos por la ley, cuya justificación pueda ser demostrada satisfactoriamente en una sociedad libre y democrática". La carga de la prueba corresponde entonces al Estado.

Los principios que sirven como base a la libertad de expresión en Canadá serían entonces los mismos que se aplicarían a la expresión y datos disponibles en Internet, con lo cual, por ejemplo, quedaría garantizado el derecho constitucional de una persona a tener acceso a los datos almacenados en la Internet y divulgarlos por esa misma vía, siempre y cuando ello no constituya una violación o amenaza a los propios datos o a las leyes aplicables en Canadá, como por ejemplo lo prescrito en el Código Penal contra la pornografía infantil, las manifestaciones de odio e incitación al terrorismo. En la sección 2(b) se incluye el derecho a ser receptor de tal expresión. Sin embargo, a falta de

circunstancias excepcionales, la sección 2(b) no constituye una garantía formal del derecho a tener acceso a información del Gobierno pues este derecho queda amparado por otras leyes.

ii. Marco legislativo

Legislación federal. Existen dos estatutos en el ámbito federal que dan lugar a regímenes bastante amplios en materia de protección de la privacidad, a saber: el Decreto de Privacidad[42/] y el Decreto de Protección de Información Personal y Documentos Electrónicos (conocida por su sigla en inglés como PIPEDA).[43/] El Decreto de Privacidad, que entró en vigor en 1983, establece las obligaciones de las instituciones del Gobierno federal con respecto a la recopilación, uso, divulgación, conservación y eliminación de información personal. Concede a los individuos el derecho a tener acceso y solicitar la corrección de información personal que el Gobierno tenga sobre ellos, salvo en los casos específicos que disponga el Decreto. Crea también la figura de un *ombudsman* independiente, conocido como Comisionado sobre Privacidad, encargado de solucionar los problemas en la materia y supervisar el cumplimiento de la ley. El Decreto de Privacidad dispone asimismo el derecho de acudir al tribunal para solicitar la revisión en un número limitado de casos. Todo lo relativo a la conservación y eliminación de información personal bajo control de instituciones de Gobierno puede encontrarse en el Decreto de Bibliotecas y Archivos de Canadá.[44/]

En el decreto PIPEDA, que entró en vigor en etapas entre 2011 y 2014, se establecen las reglas sobre la forma en que las organizaciones del sector privado pueden recopilar, utilizar o divulgar información personal en la realización de sus actividades comerciales. Quedan incluidas en esta categoría todas las organizaciones que realizan actividades comerciales o que operan en un ámbito regulado por la Federación, como es el caso de bancos, empresas de telecomunicaciones y empresas de transporte interprovincial e internacional. Las organizaciones del sector privado sujetas a la legislación provincial sobre privacidad, que ha sido reconocida por decreto como sustancialmente similar al decreto PIPEDA, están exentas del decreto federal en todo lo que se refiere a la recopilación, uso o divulgación de información personal en el ámbito intraprovincial. La ley otorga a los individuos el control sobre su información personal, obligando a las organizaciones a conseguir su consentimiento previo para poder recopilar, utilizar o divulgar su información. Los individuos también tienen el derecho a conocer y solicitar la corrección de su información personal en manos de estas organizaciones. El Decreto otorga al Comisionado de Privacidad la facultad de recibir o presentar quejas y el deber de investigar e informar sobre tales quejas, las cuales pueden ser solucionadas mediante diversos mecanismos de solución de controversias. Aquellas quejas que no puedan ser solucionadas pueden ser turnadas al Tribunal Federal, el cual tiene la facultad de ordenar a una organización que cambie sus métodos de operación y que resarza cualquier daño al peticionario.

Legislación provincial. En Canadá, todas las provincias y territorios tienen leyes que rigen la recolección, uso, divulgación y eliminación de la información personal en manos de entidades gubernamentales. Las disposiciones de tales decretos no son idénticas pero todos los estatutos se basan en los mismos principios relativos a la información. Regulan las facultades que una institución gubernamental tiene para recopilar, utilizar y difundir información personal y, por regla general,

---

42. http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html
43. http://laws-lois.justice.gc.ca/eng/acts/P-8.6/
44. http://laws-lois.justice.gc.ca/eng/acts/L-7.7/

otorga a los individuos el derecho a conocer y corregir su información personal. La tarea de supervisión queda a cargo de un comisionado independiente u *ombudsman* autorizado para recibir e investigar quejas.

En algunas provincias, una misma legislación se aplica tanto al ámbito provincial como al municipal, mientras que en otras provincias se tienen diferentes estatutos.

Algunas provincias cuentan con leyes que regulan la recopilación, uso, divulgación, conservación y eliminación de información personal por parte de organizaciones del sector privado que han sido reconocidas como sustancialmente similares al decreto PIPEDA. Algunas provincias también han aprobado leyes sobre la recolección, uso, divulgación, conservación y eliminación de información personal médica solamente y en manos de individuos u organizaciones dedicadas a la atención de la salud. Dos de estas leyes sobre privacidad en el ámbito de la salud han sido reconocidas como sustancialmente similares al decreto PIPEDA.[45/]

---

45. Alberta: Freedom of Information and Protection of Privacy Act: http://www.qp.alberta.ca/574.cfm?page=F25.cfm&leg_type=Acts&isbncln=9780779743568; Health Information Act: http://www.canlii.org/en/ab/laws/stat/rsa-2000-c-h-5/latest/rsa-2000-c-h-5.html; Personal Information Protection Act: http://www.canlii.org/en/ab/laws/stat/sa-2003-c-p-6.5/latest/sa-2003-c-p-6.5.html. Columbia Británica: Freedom of Information and Protection of Privacy Act: http://www.oipc.bc.ca/legislation/FIPPA/Freedom_of_Information_and_Protection_of_Privacy_Act(April%202010).htm; Personal Information Protection Act: http://www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm; E-Health (Personal Health Information Access and Protection of Privacy) Act: http://www.oipc.bc.ca/legislation/E-HealthLegislation/E-Health%28PersonalHealthInformationAccessandProtectionofPrivacy%29Act.mht. Manitoba: Freedom of Information and Protection of Privacy Act: http://www.gov.mb.ca/chc/fippa/act_regulation.html; Personal Health Information Act: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php. New Brunswick: Right to Information and Protection of Privacy Act: http://www.canlii.org/en/nb/laws/stat/snb-2009-c-r-10.6/latest/snb-2009-c-r-10.6.html; Personal Health Information Privacy and Access Act: http://www.canlii.org/en/nb/laws/stat/snb-2009-c-p-7.05/latest/snb-2009-c-p-7.05.html; Terranova y Labrador: Access to Information and Protection of Privacy Act: http://assembly.nl.ca/Legislation/sr/statutes/a01-1.htm; Personal Health Information Act: http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm. Territorios del Noroeste: Access to Information and Protection of Privacy Act. Nueva Escocia: Freedom of Information and Protection of Privacy Act: http://nslegislature.ca/legc/statutes/freedom.htm; Part XX of the Municipal Government Act: http://www.gov.ns.ca/snsmr/muns/manuals/pdf/mga/mga20.pdf; Personal Information International Disclosure Protection Act: http://www.canlii.org/en/ns/laws/stat/sns-2006-c-3/latest/sns-2006-c-3.html. Nunavut: Access to Information and Protection of Privacy Act; Ontario: Freedom of Information and Protection of Privacy Act: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm; Municipal Freedom of Information and Protection of Privacy Act: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm; Personal Health Information Protection Act, 2004; http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm. Prince Edward Island: Freedom of Information and Protection of Privacy Act: http://www.gov.pe.ca/law/statutes/pdf/f-15_01.pdf. Quebec: Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information: http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1_A.html; Act Respecting the Protection of Personal Information in the Private Sector: http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/

iii. Habeas data

El recurso de habeas data es un derecho constitucional reconocido en varios países latinoamericanos pero no existe como tal en el sistema jurídico canadiense. Sin embargo, todas las leyes provinciales, territoriales y federales aplicables a los sectores público o privado en Canadá reconocen el derecho de todo individuo a conocer su información personal, salvo en casos muy específicos.

El Decreto de Privacidad y su reglamentación disponen los medios para conocer y corregir la información personal que esté bajo control de una institución gubernamental. La persona interesada solo tiene que presentar una solicitud formal por escrito al funcionario correspondiente de la institución gubernamental que controla su información personal. Por otro lado, aunque se aceptan las solicitudes informales, los individuos no tienen derecho a presentar una queja al Comisionado sobre Privacidad respecto de este tipo de solicitudes puesto que no fueron hechas conforme al decreto pertinente.

iv. Autoregulación

En 1996 la Asociación Canadiense de Normalización elaboró el Código Modelo para la Protección de Información Personal (Q830), el cual fue adoptado como norma nacional por el Consejo Canadiense de Normalización. En este código quedan establecidos diez principios que equilibran los derechos de privacidad de los individuos y los requerimientos de información de las organizaciones privadas, y ha sido incorporado en el decreto PIPEDA. No obstante, sigue teniendo vigencia como instrumento autorregulatorio independiente del decreto PIPEDA y puede ser utilizado como tal por las organizaciones del sector privado que no estén sujetas a este decreto o a la legislación provincial aplicable.[46/]

B. Ejecución

i. Mecanismos de ejecución

Los mecanismos de ejecución, reglamentos y procedimientos varían de una provincia a otra. Por lo general, una persona puede presentar una queja ante un comisionado de privacidad provincial y tiene derecho a llevar su caso a los tribunales. Sin embargo, las facultades de los comisionados provinciales varían de una jurisdicción a otra, lo mismo que el derecho a acudir a un tribunal.

P39_1_A.html; An Act to amend the Act respecting health services and social services, the Health Insurance Act and the Act respecting the Régie de l'assurance maladie du Québec: http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2008C8A.PDF; Saskatchewan: Freedom of Information and Protection of Privacy Act: http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf; Local Freedom of Information and Protection of Privacy Act: http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/L27-1.pdf; Health Information Protection Act: http://www.qp.gov.sk.ca/documents/english/Statutes/Statutes/H0-021.pdf; Yukon: Access to Information and Protection of Privacy Act: http://www.gov.yk.ca/legislation/acts/atipp.pdf.

46. http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code.

En el ámbito federal, el Comisionado de Privacidad de Canadá tiene como mandato el vigilar el cumplimiento tanto del Decreto de Privacidad como del decreto PIPEDA, así como recibir e investigar las quejas sobre la aplicación de estos decretos. De igual modo, puede presentar una queja cuando existan motivos razonables para investigar un asunto previsto en estos decretos y también puede llevar a cabo auditorías sobre la veracidad y los métodos de gestión de la información que utilizan las instituciones gubernamentales. Puede incluso, para ello, hacer uso de su facultad para convocar testigos y juramentarlos, así como exigir la presentación de pruebas. Una vez realizado lo anterior, debe enviar un informe con recomendaciones –no vinculantes– a las instituciones del Gobierno federal u organizaciones del sector privado a fin de que se tomen las medidas necesarias para remediar cualquier anomalía.

El Decreto de Privacidad dispone que una persona a quien se le ha negado el derecho de conocer su información personal tiene derecho a solicitar al Tribunal una revisión luego de que el Comisionado de Privacidad haya presentado el informe sobre su investigación. El Comisionado está facultado para hacer una solicitud y comparecer en representación de una persona, con su consentimiento. En cuanto a la recopilación, uso, divulgación, conservación y eliminación de información personal, el Comisionado de Privacidad puede presentar su informe y recomendaciones directamente al demandante y al Parlamento cuando considere que una institución gubernamental no ha acatado debidamente el Decreto, pero ni el Comisionado ni el demandante tienen derecho, según el Decreto, a solicitar al Tribunal que imponga sus recomendaciones en la materia.

Según el decreto PIPEDA, luego de haber recibido el informe del Comisionado, un demandante puede solicitar una audiencia al Tribunal para tratar cualquier asunto relativo a la queja presentada. El Comisionado también puede solicitar una audiencia al Tribunal, el cual está facultado para conceder una indemnización por daños y perjuicios y ordenar a una entidad que cambie sus métodos de trabajo y que informe públicamente sobre las acciones tomadas o que pretenda tomar para corregir cualquier anomalía.

Cabe destacar que la implementación del Decreto de Privacidad es también responsabilidad del Presidente del Consejo del Tesoro, quien es nombrado como ministro especial para este decreto. Como tal, es responsable de la preparación y difusión de las directrices y lineamientos sobre la ejecución del Decreto y la reglamentación relativa a la privacidad. En la actualidad estas directrices y lineamientos son emitidos con carácter de obligatorio como instrumentos de política de la Secretaría del Consejo del Tesoro (Política sobre Protección de la Privacidad) y cuatro ordenamientos (Ordenamiento sobre el número de seguro social, Ordenamiento sobre las prácticas de privacidad, Ordenamiento sobre la evaluación del impacto de la privacidad y Ordenamiento sobre solicitudes de privacidad y corrección de información personal). Los instrumentos de política disponen el monitoreo y elaboración de informes sobre la administración del Decreto y reglamentación. El cumplimiento del Decreto es monitoreado a través de informes públicos, documentos del Consejo del Tesoro, informes de desempeño departamentales, resultados de auditorías, evaluaciones, estudios y el Marco de Gestión Responsable (conocido en inglés como Management Accountability Framework o MAF) para aquellas instituciones sujetas a este. Incluyen también las sanciones que pueden ser impuestas en caso de que la Secretaría y el Presidente del Consejo del Tesoro reciban pruebas de que existen problemas en la ejecución del decreto. Las sanciones aplicables van desde la exigencia y recomendación de informes adicionales hasta la suspensión de las facultades otorgadas a los jefes de instituciones gubernamentales por el ministro designado conforme al Decreto de Privacidad. Además del Presidente del Consejo del Tesoro, como ministro designado para la administración del Decreto

de Privacidad y su reglamentación, la responsabilidad de vigilar el cumplimiento de éste en cada una de las instituciones gubernamentales corresponde en primera instancia a los jefes designados de dichas instituciones.

Cualquier contravención injustificada de las secciones 8, 7 o 2(b) de la Carta Canadiense de Derechos y Libertades puede dar lugar a la implementación de medidas correctivas conforme a la sección 24 de la Carta. La subsección 24(1) confiere a un "tribunal de jurisdicción competente" (definido jurídicamente conforme a ciertos criterios) la facultad de conceder la reparación pertinente y justa de acuerdo a las circunstancias. La subsección 24(2) permite a un tribunal que dictamine que las pruebas fueron obtenidas infringiendo o negando cualquier derecho o libertad garantizado por la Carta, excluya tales pruebas si se establece que, considerando todas las circunstancias, su admisión en el proceso constituirían el descrédito de la impartición de la justicia. Además, según la subsección 52(1) del Decreto Constitucional de 1982, cualquier ley o instrumento subordinado que se determine jurídicamente que infringe las subsecciones 8, 7 o 2(b) de la Carta serán declarados sin vigencia ni efecto a menos que el Estado justifique que tal restricción constituye una limitación razonable en una sociedad libre y democrática.

ii. Protección de datos/autoridades ejecutoras

En el ámbito federal, la principal autoridad responsable de ejecutar las leyes en materia de protección de datos es el Comisionado de Privacidad de Canadá, quien es agente del Parlamento, independiente del Ejecutivo y de las instituciones de Gobierno que son objeto de sus investigaciones y auditorías. Este Comisionado es nombrado por un período de siete años por el Gobernador, con la aprobación por resolución tanto del Senado como de la Cámara de los Comunes. Ocupa su puesto mientras observe buena conducta y solo puede ser removido de su cargo por instrucciones del Senado y de la Cámara de los Comunes. "Cumplirá exclusivamente los deberes del cargo de Comisionado de Privacidad" e informar a anualmente sobre sus actividades al Parlamento aunque podría pedírsele que lo haga con mayor frecuencia en situaciones de emergencia. Su nombramiento podrá ser renovado al cabo del período de siete años. La Oficina del Comisionado de Privacidad cuenta con aproximadamente 176 empleados a su cargo y un presupuesto anual de cerca de 24 millones de dólares canadienses.[47/]

En los últimos cinco años, el Comisionado de Privacidad de Canadá ha recibido un promedio de 750 quejas al año relacionadas con el Decreto de Privacidad, y cerca de 330 quejas al año relacionadas con el decreto PIPEDA.[48/]

Conforme al Decreto de Privacidad, el Comisionado recibirá e investigará cada queja que se le presente. Según el decreto PIPEDA, está autorizado para tratar algunas quejas de manera sumaria. De hecho, se le permite negarse a investigar una queja si, por ejemplo, la parte demandante podría haber solicitado su revisión o entablado primero otros recursos a su disposición, o si convendría mejor que la queja fuese sujeta a otros procedimientos conforme a otra ley. Del mismo modo, el Comisionado podría suspender las investigaciones en un cierto número de circunstancias limitadas,

47. Comisionado de Privacidad de Canadá: http://www.priv.gc.ca/
48. Annual Report on the Personal Information and Electronic Documents Act (2010): http://www.priv.gc.ca/information/ar/201011/2010_pipeda_e.pdf; Annual Report on the *Privacy Act* (2010-2011): http://www.priv.gc.ca/information/ar/201011/201011_pa_e.pdf.

incluso cuando considere que existen pruebas insuficientes para seguir adelante con la investigación, si la queja es trivial, frívola, irritante o hecha de mala fe, o si el asunto ya es objeto de otra investigación en curso, etc.

En el ámbito provincial, en cada provincia y territorio existe un comisionado de privacidad independiente, responsable principalmente de hacer cumplir las leyes relativas a la protección de datos pero el número de personal y la magnitud del presupuesto con que cuenta varía considerablemente.[49/]

Conforme al Decreto de Privacidad, el Comisionado y cualquier persona que actúe en su representación o bajo sus instrucciones preserverá el carácter confidencial de toda información de que tenga conocimiento en el desempeño de sus deberes y funciones. No obstante, el Comisionado está autorizado para divulgar tal información si, en su opinión, es necesario para llevar a cabo una investigación al amparo del Decreto.

El decreto PIPEDA prohíbe al Comisionado, o a cualquier persona que actúe en su representación, divulgar cualquier información de que tenga conocimiento en el desempeño de los deberes y facultades que le otorga este decreto. El Comisionado puede, sin embargo, hacer pública información sobre la gestión de una organización si considera que es en beneficio del público.

El Comisionado está autorizado para divulgar cierta información a sus contrapartes extranjeras siempre y cuando éstas tengan, conforme a las leyes de sus respectivos países, 1) funciones y deberes similares a los del Comisionado de Privacidad con respecto a la protección de datos personales, y 2) la responsabilidad de intervenir en aquellos casos que se considere contravengan el decreto PIPEDA.

Tal información 1) debe ser pertinente a una posible investigación en curso sobre una contravención de una ley extranjera, siempre y cuando el hecho objeto de investigación sea considerablemente similar a aquel que sería considerado en contravención del decreto PIPEDA, o 2) debe ser divulgada para que el Comisionado de Privacidad obtenga de sus contrapartes extranjeras información que sería útil para una investigación o auditoría que se lleve a cabo al amparo del decreto PIPEDA.

---

49. Office of the Information and Privacy Commissioner of Alberta: http://www.oipc.ab.ca/pages/home/default.aspx; Office of the Information and Privacy Commissioner for British Columbia: http://www.oipc.bc.ca; Ombudsman of Manitoba : http://www.ombudsman.mb.ca; Access to Information and Privacy Commissioner of New Brunswick: http://www2.gnb.ca/content/gnb/en/contacts/dept_renderer.201145.html; Information and Privacy Commissioner of Newfoundland and Labrador: http://www.oipc.nl.ca; Information and Privacy Commissioner of the Northwest Territories: http://www.commissioner.gov.nt.ca/privacy; Nova Scotia Freedom of Information and Protection of Privacy Review Office: http://www.foipop.ns.ca; Information and Privacy Commissioner of Nunavut: http://www.info-privacy.nu.ca; Office of the Information and Privacy Commissioner of Ontario: http://www.ipc.on.ca/english/Home-Page; Information and Privacy Commissioner of Prince-Edward Island: http://www.assembly.pe.ca/index.php3?number=1013943; Commission d'accès à l'information du Québec: http://www.cai.gouv.qc.ca/index-en.html; Information and Privacy Commissioner of Saskatchewan: http://www.oipc.sk.ca; Information and Privacy Commissioner of Yukon: http://www.ombudsman.yk.ca/privacy/ipchome.html.

El Comisionado podrá divulgar información a sus contrapartes extranjeras solo si se ha establecido un convenio por escrito.

iii. Recursos

Recurso. En varias provincias canadienses, la legislación ha hecho ilícito el acto de invasión de la privacidad. El derecho a la privacidad también existe en el Código Civil de Quebec. En varias provincias, los individuos pueden solicitar el resarcimiento por violaciones a la privacidad. En otras provincias regidas por el derecho consuetudinario, el recurso depende de que los tribunales reconozcan la violación a la privacidad. El Tribunal de Apelaciones de Ontario introdujo recientemente este recurso al reconocer un acto ilícito de "intrusión en la intimidad". [*Véase* Jones v. Tsige, (2012) ONCA 32.]

En el ámbito federal, el Decreto de Protección de Datos Personales y Documentos Electrónicos permite expresamente al tribunal ordenar el pago de daños al demandante, incluidos cualesquiera daños por cualquier humillación que haya sufrido.[50/]

El recurso por daños causados por la violación de la privacidad por parte de una institución federal no ha quedado claramente establecido en el Decreto de Privacidad. En consecuencia, este recurso depende de que los tribunales reconozcan la violación a la privacidad.

Como se indicó en la subsección anterior, la Carta dispone algunos recursos internos. Una persona puede recurrir al amparo de la sección 24 de la Carta en los casos en que se haya infringido el derecho garantizado por las secciones 8, 7 o 2(b). Entre los posibles recursos está el pago de daños y la exclusión de pruebas que hayan sido obtenidas violando los derechos constitucionales. De igual manera, cuando las leyes entren en conflicto con la Carta, pueden ser declaradas sin valor ni efecto conforme a la subsección 52(1) del Decreto Constitucional de 1982.

Autoridad encargada de la protección de datos. Tal como se mencionó anteriormente, las legislaciones provincial y federal son ejecutadas por intermedio de los parlamentos, los comisionados de privacidad y los tribunales. *Véase* nuestra respuesta a la pregunta IIA, en donde se encontrará una descripción de las modalidades de aplicación de las leyes en el ámbito federal.

iv. Capacidades de investigación/procesamiento penal

Según el Decreto de Privacidad, el Comisionado de Privacidad de Canadá está facultado para recibir una queja relacionada con temas tales como el uso y difusión de datos personales o el derecho de las personas a conocer su información personal. En caso de que el Comisionado esté convencido de que existen razones suficientes para investigar uno de estos temas podrá iniciar una demanda. De igual forma y a su entera discreción, puede llevar a cabo una investigación con respecto a la información de carácter personal que esté bajo el control de instituciones gubernamentales para cerciorarse de que se cumpla lo dispuesto con la recopilación, uso y difusión de este tipo de datos.

---

50 Nammo v. TransUnion of Canada Inc., (2010) FC 1284; Girao v. Zarek Taylor Grossman Hanrahan LLP, (2011) FC 1070 y Landry v. Royal Bank of Canada, (2011) FC 687).

Posteriormente, emitirá un informe con los resultados de su investigación y cualquier recomendación que considere pertinente.

Según el decreto PIPEDA, además de estar facultado para investigar quejas según lo descrito en la sección D anterior, el Comisionado de Privacidad de Canadá puede entablar una demanda si considera que existen razones suficientes para investigar un asunto amparado por este decreto. El Comisionado tiene un año para presentar un informe sobre cualquier demanda que haya iniciado. Este informe debe también contener los resultados de la investigación y recomendaciones del Comisionado, una nota sobre el acuerdo al que hayan llegado las partes y, en caso de que sea pertinente, una nota sobre cualquier acción tomada o propuesta para poner en práctica sus recomendaciones. El Comisionado también puede auditar los métodos que usa una organización para la gestión de información personal si considera que existen razones suficientes para creer que dicha organización está contraviniendo el Decreto. Luego de la auditoría, el Comisionado deberá entregar a dicha organización una copia de su informe con los resultados de su auditoría y cualquier recomendación que considere pertinente. Este informe puede también ser incluido en el informe anual que presenta el Comisionado al Parlamento.

El decreto PIPEDA no incluye sanciones penales. Sin embargo, según éste, el Comisionado puede divulgar información en el curso de una demanda por un delito de perjurio contemplado en el Código Penal de Canadá con respecto a una declaración hecha al amparo del decreto PIPEDA. El Comisionado puede asimismo revelar al Procurador General de Canadá o a los procuradores generales provinciales información relativa a la comisión de un delito conforme a las leyes de Canadá o de una provincia, si es que el Comisionado opina que existen pruebas suficientes para hacerlo[51/].

C. Cooperación transfronteriza

i. Transferencia de datos

En el ámbito federal, las reglas son diferentes pues todo depende de si se aplica el Decreto de Privacidad o el decreto PIPIDA. El primero de éstos no establece reglas ni condiciones especiales para la divulgación de datos personales a otros países. Las mismas reglas específicas y limitadas que rigen la divulgación de datos personales a terceras partes, aplicables en el ámbito nacional, también se aplican a otros países. No obstante, el Gobierno federal ha establecido una serie de directrices para las instituciones sujetas al Decreto de Privacidad, que incluye una lista de elementos sobre privacidad y algunos criterios encaminados a tomar en cuenta la privacidad antes de establecer cualquier contrato, en particular, si éste implica la transmisión de datos allende las fronteras del país.[52/]

El decreto PIPEDA contiene un principio mediante el cual la entidad que controla o custodia datos personales es responsable de ellos, incluso de aquellos que haya transferido a terceros para su procesamiento. Cualquier entidad sujeta al decreto PIPEDA debe contar con los medios contractuales o afines para asegurarse de que los datos que hayan transmitido a terceros para su procesamiento sean protegidos por esas terceras partes en la misma medida que establece el mencionado decreto. Este requerimiento es válido tanto si el procesador de datos se encuentra en Canadá como en el extranjero.

---

51. Código Penal, secciones 56.1, 368(1) y 402.2 sobre robo de identidad y delitos conexos: http://laws-lois.justice.gc.ca/eng/acts/C-46.
52. Documento guía: Taking Privacy into Account Before Making Contracting Decisions: http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcptb-eng.asp

En el ámbito provincial, la divulgación de datos personales en manos de entidades de gobierno provinciales o territoriales a otros países es regulada por los respectivos estatutos provinciales o territoriales. Las limitaciones o condiciones a tales transferencias varían de una provincia o territorio a otro.

ii. Instrumentos/acuerdos internacionales

Canadá es signatario de las Directrices que Rigen la Protección de la Privacidad y de los Flujos Transfronterizos de Datos Personales, de la OCDE de 1984. Los estatutos que regulan la protección de datos personales en el ámbito federal –el Decreto de Privacidad y el decreto PIPEDA– fueron ambos adoptados con el ánimo de acatar las directrices de la OCDE.

Canadá es miembro del APEC desde 1989 y aprobó las Directrices de Privacidad del APEC en 2004 y el Sistema de Reglas Transfronterizas sobre Privacidad de este mismo foro en 2011. La Oficina del Comisionado de Privacidad de Canadá unió esfuerzos con entidades similares en todo el mundo en septiembre de 2010 para crear la red GPEN. El Comisionado también participa en el acuerdo CPEA del APEC.

En diciembre de 2001, la Comisión Europea determinó que el decreto PIPEDA fuese reconocido con el grado de "suficiencia", lo cual significa que satisface las normas de protección de datos personales especificados en la Directiva sobre Protección de Datos de la Unión Europea. Esta decisión fue confirmada en 2006 luego de que se hiciera una evaluación del grado de cumplimiento de Canadá conforme a la decisión adoptada en 2001.[53/] En 2005, también se consideró adecuada la protección de datos personales contenidos en el Registro de Pasajeros Aéreos transferidos a la Dirección General de Servicios Fronterizos.[54/]

iii. Cooperación transfronteriza en materia de investigación y ejecución de las leyes

La colaboración transfronteriza se da entre algunas instituciones federales y sus contrapartes en otros países.

El Comisionado de Privacidad colabora con sus contrapartes en algunas investigaciones sobre la transferencia de datos personales entre países. El Comisionado es miembro fundador de la red GPEN, creada para facilitar el intercambio de información sobre temas relacionados con la

---

53. Decisión de la Comisión del 20 de diciembre de 2001 conforme a la Directriz 95/46/EC del Parlamento Europeo y del Consejo sobre la protección adecuada de datos personales establecida en el decreto PIPEDA de Canadá. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0002:en:NOT;
La aplicación de la Decisión de la Comisión 2002/2/EC del 20 de diciembre de 2001 conforme a la Directriz 95/46/EC del Parlamento Europeo y del Consejo sobre la protección adecuada de datos personales establecida en el decreto PIPEDA de Canadá. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0002:en:NOT;
http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-5.
54. Decisión de la Comisión del 6 de septiembre de 2005 sobre la adecuada protección de datos personales contenidos en el Registro de Pasajeros Aéreos transferidos a la Dirección General de Servicios Fronterizos: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-5.

ejecución de las leyes y las actividades de colaboración. El Comisionado es también participante del acuerdo CPEA del APEC, en el que se disponen de mecanismos para facilitar la cooperación transfronteriza en la aplicación de leyes sobre privacidad, incluso facilitar el contacto entre los participantes del CPEA con el propósito de buscar asistencia o referencias sobre investigaciones relativas a la privacidad o asuntos relacionados con la aplicación de las leyes.

Además, cuando se requiere, las autoridades policiacas cooperan con otros gobiernos en asuntos relacionados con la ejecución del Código Penal en materia de robo de identidad y otras infracciones específicas relacionadas con la protección de datos.

D. Jurisprudencia y retos especiales

En los ámbitos federal y provincial, la protección de datos personales está regida principalmente por los estatutos. En consecuencia, los jueces influyen en gran medida en las leyes que regulan la protección de la privacidad individual, ya sea en el contexto del análisis jurídico de cualquier impugnación que se haga de las decisiones gubernamentales o en el contexto de la interpretación de los estatutos que dan lugar a los regímenes de protección de la privacidad.[55/]

Las decisiones de índole judicial sobre el alcance y aplicación de la sección 8 de la Carta desempeñen ciertamente un papel importante en la protección de la privacidad de la persona en Canadá.[56/]

El desarrollo de nuevas tecnologías, en particular la computadora, con su poder casi ilimitado para recopilar, usar, diseminar y conservar datos, fue lo que impulsó la adopción tanto del Decreto de Privacidad como del decreto PIPEDA. Estos dos decretos fueron redactados con un lenguaje neutral desde el punto de vista tecnológico y por ello ha sido posible encontrar la forma de aplicar los principios de protección de la privacidad a las nuevas tecnologías y servicios que han surgido desde que fueron adoptados.

---

55. Dagg vs. Canada (Ministro de Finanzas), [1997] 2 S.C.R. 403; H.J. Heinz Co. of Canada Ltd. v. Canada (Procurador General), [2006] 1 S.C.R. 441; Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police), [2003] 1 S.C.R. 66: http://csc.lexum.org/en/2003/2003scc8/2003scc8.html.
56. Hunter v. Southam Inc., [1984] 2 S.C.R. 145: http://csc.lexum.org/en/1984/1984scr2-145/1984scr2-145.html; R. v. Dyment, [1988] 2 S.C.R. 417: http://scc.lexum.org/en/1988/1988scr2-417/1988scr2-417.html; R. v. Plant,[1993] 3. S.C.R. 281: http://scc.lexum.org/en/1993/1993scr3-281/1993scr3-281.html; R. v. Colarusso, [1994] 1 S.C.R. 20: http://scc.lexum.org/en/1994/1994scr1-20/1994scr1-20.html; Smith v. Canada (Procurador General), [2001] 3 S.C.R. 902: http://scc.lexum.org/en/2001/2001scc88/2001scc88.html;
R. v. Law, [2002] 1 S.C.R. 227: http://scc.lexum.org/en/2002/2002scc10/2002scc10.html; R. v. Tessling, [2004] 3 S.C.R. 432: http://scc.lexum.org/en/2004/2004scc67/2004scc67.html; R. v. Rodgers, [2006] 1 S.C.R. 554: http://scc.lexum.org/en/2006/2006scc15/2006scc15.html; R. v. Kang-Brown, [2008] 1 S.C.R. 456: http://scc.lexum.org/en/2008/2008scc18/2008scc18.html; R. v. A.M., [2008] 1 S.C.R. 569: http://scc.lexum.org/en/2008/2008scc19/2008scc19.html; R. v. Patrick, [2009] 1 S.C.R. 579: http://scc.lexum.org/en/2009/2009scc17/2009scc17.html; R. v. Gomboc, [2010] 3 S.C.R. 211: http://csc.lexum.org/en/2010/2010scc55/2010scc55.html.

3. Colombia

Las respuestas de Colombia al Cuestionario de Legislación y Prácticas sobre Privacidad y Protección de Datos de la CAJP se encuentran en el documento CP/CAJP-3026/11 add. 10, y constituyen la base para la información que se resume en esta sección.[57/]

A. Contexto jurídico

i. Marco constitucional

La Constitución de 1991 establece que 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.[58/] La Constitución garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación, y garantiza que no habrá censura. Establece que estos son libres y que tienen responsabilidad social. Además garantiza el derecho a la rectificación en condiciones de equidad.[59/] También, dado que tanto el derecho a la privacidad como el derecho a la libertad de expresión están consagrados en el capítulo I (sobre derechos fundamentales) de la Constitución, son de aplicación inmediata.[60/]

ii. Marco legislativo

El Congreso colombiano aprobó la ley estatutaria que contiene "disposiciones generales para la protección de datos personales" el 16 de diciembre de 2010 (la "nueva ley"). Su entrada en vigor requería una revisión por parte de la Corte Constitucional, lo cual ocurrió el 6 de octubre de 2011[61/], así como una resolución por escrito de la Corte y la ratificación del Presidente, lo cual no ha ocurrido a la fecha del presente informe aunque se espera que ocurra.

---

57. El Congreso de la República de Colombia aprobó la Ley sobre Protección de Datos en diciembre de 2010, y antes de entrar en vigor debe ser estudiada por la Corte Constitucional, la cual dictaminó su constitucionalidad el 6 de octubre de 2011 pero a la fecha en que se elaboró este informe no ha emitido su resolución final, necesaria para que esta ley pueda ser sancionada por el Presidente. Por lo tanto, las respuestas al cuestionario y el contenido de esta sección se limitan exclusivamente a la texto de la ley. A la fecha de este informe no existe jurisprudencia ni aspectos prácticos/regulatorios con respecto a la implementación de la ley.
58. Artículo 15 de la Constitución.
59. Artículo 20.
60. Artículo 85 de la Constitución.
61. Revisión constitucional en Sentencia C-748-2011.

El Congreso modificó también el Código Penal, con lo cual se crea un nuevo bien jurídico tutelado, denominado "protección de la información y de los datos". De esta forma se establecen nuevos delitos penales relacionados con el uso de computadoras, la protección de la información y la protección de datos personales, y se establecen penas de cárcel hasta de 120 meses y multas de hasta 1500 veces el salario mínimo legal vigente.[62/]

La ley sanciona específicamente la violación de datos personales cuando una persona/entidad, sin autorización y en beneficio propio o de un tercero, obtiene, compila, sustrae, ofrece, vende, intercambia, envía, compra, intercepta, difunde, modifica o utiliza códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios similares con pena de prisión de 48 a 96 meses y con multa 100 a 1000 salarios mínimos legales mensuales vigentes.

La Ley 1266 promulgada en 2008 establece también las disposiciones generales del habeas data y regula el manejo de la información contenida en bases de datos personales, en particular las de carácter financiero, crediticio, mercantil y de información, así como la información de terceros países.[63] / Por último la Ley 79, promulgada en 1993, regula el levantamiento del censo a nivel nacional y establece los procedimientos para procesar los datos personales en ese contexto.

62. Ley 1429 de 2010.
63. En su revisión, la Corte Constitucional determinó que la Ley 1266 era de naturaleza sectorial y la limita exclusivamente al procesamiento de datos relacionados con el análisis de riesgo crediticio (Sentencia C-1011).

Las leyes 1266, 1273 y la recientemente aprobada Ley de Protección de Datos Personales aplican a entidades tanto públicas como privadas. La Ley 79 se aplica exclusivamente a la entidad encargada de realizar los censos públicos.

iii. Habeas data

En el ámbito constitucional, como se indicó en la subsección (i) anterior, el recurso conocido comúnmente como "habeas data" establece que los individuos tienen derecho a su intimidad personal y familiar y a su buen nombre. El Estado debe respetar este derecho y garantizar que sea respetado por otros. El individuo tiene de igual modo derecho a conocer, actualizar y rectificar los datos que se hayan recogido sobre él en bancos de datos y en archivos públicos y privados.[64/]

En el ámbito estatutario, la nueva ley de protección de datos hace operativo el derecho constitucional de todos los individuos a conocer, actualizar y corregir datos personales en bases de datos o archivos, sean estos públicos o privados.[65/] Además, en su revisión de la ley, la Corte Constitucional estableció que la constitucionalidad de la nueva ley de protección de datos establece que los individuos tienen derecho a borrar esa información, creando así cierto paralelismo con los derechos a acceder, rectificar, cancelar y oponerse (ARCO) al procesamiento de datos personales.[66/]

iv. Autoregulación

La nueva ley de protección de datos permite el desarrollo de sistemas de autoregulación o autocontrol como el de las Normas Corporativas Vinculantes. Este sistema estaría sujeto a la reglamentación que expida el Gobierno en el futuro con el objetivo de certificar las buenas prácticas en protección de datos personales y su transferencia a terceros países[67/]

B. Ejecución

i. Mecanismos de ejecución

El principal mecanismo para poner en práctica está contenido en la Ley 2591 de 1991 y en las disposiciones relativas a la protección de datos mencionadas anteriormente. Tanto la Ley 1266 de 2008 como la nueva ley de protección de datos establecen por vía administrativa el procedimiento de consulta que procede ante el responsable o encargado del tratamiento o el de reclamo que procede directamente ante la autoridad de control. Para ejercer este último, debe haberse primero surtido el proceso de consulta en caso de que el titular considere que se está dando algún tipo de vulneración en el tratamiento de su información.

En parte, la nueva ley de protección de datos dispone que la persona puede consultar y conocer su información personal en cualquier base de datos pública o privada. La consulta será hecha utilizando el procedimiento dispuesto por el procesador de los datos, y será atendida en un plazo máximo de 10 días hábiles a partir de la fecha de recepción. Cuando no sea posible atender la solicitud de consulta en el plazo indicado, el procesador informará a la persona las razones del retraso

64. Artículo 15 de la Constitución.
65. Nueva ley, artículo 1.
66. Sentencia de la Corte Constitucional C-748 de 2011.
67. Nueva ley, artículo 28.

y la fecha en que se le atenderá. En cualquier caso, el retraso no excederá cinco días hábiles después del vencimiento del primer plazo.[68/]

ii. Protección de datos/autoridades ejecutoras

En la actualidad existen en Colombia dos autoridades administrativas responsables de la ejecución de las leyes y normas sobre privacidad/protección de datos: (i) la Superintendencia de Industria y Comercio y (ii) la Superintendencia Financiera.

La Superintendencia de Industria y Comercio es un organismo de carácter técnico, adscrito a la Rama Ejecutiva del Poder Público –Ministerio de Comercio, Industria y Turismo–, entre cuyas funciones se incluye la de velar por el cumplimiento de las normas sobre protección del consumidor, protección de datos personales, cumplimiento con las normas de competencia/antimonopolio, gestión del sistema nacional de propiedad industrial, así como asuntos jurisdiccionales en materia de protección al consumidor y competencia desleal.[69/] Dentro de la Superintendencia, la Delegatura para la Protección de Datos Personales vela por el cumplimiento de las leyes referentes al procesamiento de datos personales.[70/] La Superintendencia de Industria y Comercio tiene 599 funcionarios, su presupuesto en 2012 ascendió a 56.396.350.000 pesos colombianos para operación y 13.242.180.000 pesos colombianos para inversión.

La Superintendencia Financiera es un organismo de carácter técnico, adscrito a la Rama Ejecutiva del Poder Público –Ministerio de Hacienda y Crédito Público– encargada de supervisar el funcionamiento de los mercados financiero y bursátil de Colombia, preservar su estabilidad, seguridad y confianza, así como promover, organizar y desarrollar el mercado de valores y la protección de los inversionistas, ahorradores y asegurados.[71/]

En términos generales, la Superintendencia de Industria y Comercio atiende por sí sola las quejas que le presentan individuos y determina, con base en ellas, si el caso amerita abrir una investigación administrativa. No obstante, cabe destacar que la Superintendencia tiene también amplias facultades para impartir instrucciones, realizar auditorías externas o llevar a cabo investigaciones oficiales por iniciativa propia.

El volumen de quejas atendidas por la Superintendencia de Industria y Comercio sobre violación de las normas de protección de datos y, en particular, las disposiciones de la Ley 1266 de 2008 es el siguiente: 654 en 2009; 1058 en 2010; 1725 en 2011; 228 de enero a marzo de 2012. El total a la fecha de este informe era de 3665.

---

68. Artículo 14.
69. Decreto 4886 de 2011.
70. La Delegatura para la Protección de Datos Personales fue incorporada a la estructura de la Superintendencia de Industria y Comercio mediante el Decreto 4886 de 2011.
71. Colombia no proporcionó cifras sobre el personal y el presupuesto de la Superintendencia Financiera.

iii. Recursos

La persona que considere que los datos personales contenidos en una base de datos pública o privada deban ser corregidos, actualizados o borrados, puede presentar una queja ante el procesador de los datos. Dicha queja se hará por escrito y en ella se identificará al titular de la información y se definirán los hechos que la sustentan. Luego de haber recibido la queja, el procesador de los datos deberá anotar "queja pendiente" en la base de datos y deberá atenderla en un plazo de 15 días hábiles a partir de su recepción.[72/] Si después de haber completado este proceso, la persona considera que la queja no ha sido atendida adecuadamente, podrá elevar su queja a la Superintendencia de Industria y Comercio.[73/]

Asimismo la Ley 1266 establece varias facultades para la Superintendencia de Industria y Comercio sobre la privacidad/protección de datos, incluidas las de impartir instrucciones y órdenes sobre la forma en que los procesadores de datos deben cumplir las disposiciones de la ley, normas y regulaciones de privacidad/protección de datos; velar y garantizar el cumplimiento de las disposiciones de las leyes, normas y regulaciones de protección de datos, así como las instrucciones impartidas por la respectiva Superintendencia; velar porque los procesadores de datos tengan los sistemas de seguridad y capacidades técnicas suficientes para garantizar que no se alteren ni se pierden los datos personales, ni sean consultados ni utilizados sin autorización conforme lo previsto en la ley; ordenar la realización de auditorías externas para verificar que los procesadores de datos cumplan las disposiciones de la ley; ordenar de oficio o a petición de una persona la modificación o eliminación de datos personales cuando ello sea procedente, conforme lo establecido en la ley; iniciar de oficio o a petición de una persona investigaciones administrativas contra los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, con el fin de establecer si existe responsabilidad administrativa derivada del incumplimiento de las disposiciones de la ley o de las órdenes o instrucciones impartidas por el organismo de vigilancia respectivo, y, si es el caso, imponer sanciones u ordenar las medidas que resulten pertinentes para que se respeten los derechos a la privacidad/protección de datos.[74/]

iv. Capacidades de investigación/procesamiento penal

Según se indicó anteriormente, la Ley 1266 permite a las autoridades encargadas de la aplicación iniciar investigaciones de oficio o a petición de una de las partes. Los procedimientos penales son competencia del Procurador General. Al respecto, la Ley 1273, mediante la que se modifica el Código Penal, establece la creación de un nuevo bien jurídico tutelado, denominado "protección de la información y de los datos" y que está detallado en dos capítulos. Un capítulo contra ataques a la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos y de atentados informáticos y otras infracciones; y un segundo capítulo en el que se establecen los tipos de delitos relativos a la protección de datos personales.[75/]

Con respecto a la violación de datos personales, el código dispone que cuando una persona/entidad, sin autorización y en beneficio propio o de un tercero, obtiene, compila, sustrae, ofrece, vende, intercambia, envía, compra, intercepta, difunde, modifica o utiliza códigos personales

72. Artículo 15.
73. Artículo 16.
74. Ley 1266 de 2008, artículo 17.
75. Código Penal, Título VII BIS.

o datos personales contenidos en ficheros, archivos, bases de datos o medios similares puede ser sancionado con pena de prisión de 48 a 96 meses y con multa 100 a 1000 salarios mínimos legales mensuales vigentes.

Al respecto, es importante aclarar que la Ley 1266 definió el término dato personal como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica". Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.[76/]

C. Cooperación transfronteriza

i. Transferencia de datos

La nueva ley de protección de datos prohíbe la transferencia de datos personales a países que no brinden la protección adecuada que determina la Superintendencia de Industrial y Comercio. En ningún caso las normas del receptor no podrán ser inferiores a las normas establecidas por las leyes colombianas.[77/]

ii. Instrumentos/acuerdos internacionales

Aunque lo permite la nueva ley, no se han dado casos de participación formal en instrumentos o acuerdos internacionales. No obstante, Colombia es parte de la RIPD y a través de ella ha participado en el intercambio de información, inquietudes y sugerencias con respecto a los problemas más recientes sobre la protección de datos en los ámbitos global y latinoamericano.

Colombia no ha recibido la certificación de la Unión Europea. Solicitó a la Comisión Europea que iniciara el proceso de adaptación en 2009 pero éste fue suspendido mientras se redactaba y adoptaba la nueva ley de datos personales. Se espera que Colombia vuelva a solicitar la iniciación del proceso en abril de 2002.

iii. Cooperación transfronteriza en materia de investigación y ejecución de las leyes

La nueva ley de protección de datos establece que la autoridad correspondiente solicitará la colaboración de entidades internacionales o extranjeras cuando se vean afectados los derechos de ciudadanos colombianos.[78/] La nueva ley no prescribe la colaboración con otros países, pero dado que aún no entra en vigor esta facultad la ejerce la autoridad en la práctica.

---

76. Sección 269F: Violación de datos personales
77. Artículo 26. La ley establece excepciones para los casos en que la persona haya dado su consentimiento para la transferencia; para el intercambio de datos médicos necesarios para un tratamiento o por razones de salud pública; para transferencias bursátiles o bancarias; para transferencias acordadas en el marco de un tratado internacional; para salvaguardar el bien público o para el establecimiento, ejercicio o defensa de un derecho en un proceso judicial.
78. Artículo 21.

D. Jurisprudencia y retos especiales

Desde 1992, la Corte Constitucional ha expedido alrededor de 70 sentencias en relación con temáticas sobre protección de datos personales.[79/] Entre los temas más importantes considerados por la Cortes se incluyen los siguientes: la dignidad humana y privacidad conforme a la Constitución de 1991; los efectos jurídicos de las nuevas tecnologías en las libertades personales; la privacidad, el habeas data y la aplicación del artículo 15 de la Constitución; la correlación entre privacidad y el derecho a conocer información; los datos como "propiedad"; bases de datos y derecho constitucional; la caducidad de datos personales; la creciente informatización e insuficiente protección legal y social; el uso responsable de la información, etc. Entre los retos más importantes que enfrenta Colombia en la implementación de su nueva ley sobre protección de datos se incluye la informática en nube y los flujos transfronterizos de información.

Costa Rica

Las respuestas de Costa Rica al Cuestionario de Legislación y Prácticas sobre Privacidad y Protección de Datos de la CAJP se encuentran en el documento CP/CAJP-3026/11 add. 6, y constituyen la base para la información que se resume en esta sección.

A. Contexto jurídico

i. Marco constitucional

La Constitución de Costa Rica de 1949 establece el derecho a la intimidad, la libertad y el secreto de las comunicaciones. Según el artículo 24 de la Constitución de Costa Rica, los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes del país son considerados inviolables. Esta disposición abarca diversas manifestaciones de la vida privada (económicas, comerciales, financieras y profesionales) que únicamente podrían divulgarse a terceros si existe un evidente interés público en esa información. La existencia de ese interés público es el elemento que distingue entre la información pública, la cual es de acceso general, y la información privada, la cual debe ser declarada confidencial.[80/]

El derecho a la libertad de expresión queda consagrado en el artículo 28 de la Constitución y garantiza que ninguna persona puede ser inquietada ni perseguida por expresar sus opiniones ni por acto alguno que infrinja la ley. De igual manera, el artículo 29 establece que todos los ciudadanos pueden comunicar sus pensamientos de palabra o por escrito, y publicarlos sin previa censura, aunque los hace responsables de los abusos que cometan en el ejercicio de este derecho.

La autodeterminación informativa es un derecho nuevo, nacido del advenimiento de las tecnologías de la información y las comunicaciones. En consecuencia, a diferencia de otros países, la Constitución de Costa Rica de 1949 no incluye disposición alguna que trate específicamente sobre la

---

79. Esta extensa jurisprudencia se resume en el cuadro que aparece en la sección III del documento que contiene las respuestas de Colombia al Cuestionario de Legislación y Prácticas sobre Privacidad y Protección de Datos (CP/CAJP-3026/11 add. 10), disponible en: http://www.oas.org/dil/esp/proteccion_de_datos_cuestionario_Colombia.pdf.
80. Artículo 24.

privacidad/protección de datos ni el habeas data. Sin embargo, cabe hacer notar que los académicos, jueces y operadores jurídicos intentan interpretar los artículos constitucionales mencionados anteriormente en materia de protección de la privacidad e intimidad con el propósito de hallar sustento al derecho a la autodeterminación informativa (protección de datos y habeas data), pero el alcance de los derechos es más amplio e importante que esto último.

ii. Marco legislativo

Legislación de amplio alcance: El 7 de julio de 2011 se aprobó en Costa Rica la Ley N.º 8968, "Protección de la persona frente al tratamiento de sus datos personales", aplicable en el ámbito nacional (incluidos los estados y municipios), tanto para el sector público como privado. Se trata de un cuerpo normativo que procura recoger los principios internacionalmente reconocidos de la autodeterminación informativa, establecer una amplia base de aplicación y proporcionar una definición de los diferentes elementos que abarca. Incluye también los principios y derechos básicos en cuanto a la protección de datos personales, tales como la explicación del contenido de la autodeterminación informativa, los principios del consentimiento informado, la obligación de informar al ciudadano, la necesidad de contar con el consentimiento del interesado, algunas excepciones a la autodeterminación informativa, desarrolla el principio de la calidad de la información, incluida la actualidad, la veracidad, la exactitud y la adecuación al fin de la recopilación de datos.

Contiene también otros derechos que asisten a los ciudadanos, tales como el acceso a la información (que incluye la existencia de datos personales en bases de datos públicas o privadas) y el

derecho de rectificación. Trata también de las distintas categorías de datos, tales como lo que se entenderá por datos confidenciales, datos personales de acceso restringido, datos personales de acceso irrestricto y datos referentes al comportamiento crediticio.

La ley regula además la seguridad y confidencialidad en el tratamiento de los datos, así como protocolos de actuación sobre los procedimientos que deberán seguirse en la recolección, almacenamiento y manejo de los datos personales, y garantías necesarias de protección contra actos que violen los derechos fundamentales de los ciudadanos. Tiene también una referencia a la transferencia de datos personales, que en regla general, solo podrá realizarse cuando el titular del derecho haya autorizado expresa y válidamente tal acción y ello se efectúe sin vulnerar los principios y derechos reconocidos en esta ley.

Legislación sectorial. Existe también cierta reglamentación sectorial relacionada con la privacidad/protección de datos, en la que queda incluida la Ley General de Telecomunicaciones N.º 8642, que trata de la privacidad de las comunicaciones y la protección de los datos personales que pueden estar en manos de compañías que presten servicios de telecomunicaciones y que exige que tales compañías tengan las medidas técnicas necesarias para garantizar la seguridad de las redes y servicios, el derecho a la intimidad y la protección de los datos personales de los abonados[81/]; el Reglamento sobre Medidas de Protección de la Privacidad al que están sometidos todos los operadores o proveedores de servicios de telecomunicaciones con la finalidad de garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos personales de los usuarios[82/]; la Ley Reguladora del Contrato de Seguros N.º 8956, que contempla la protección que debe darse a los datos recabados y la exigencia a las entidades aseguradoras, subsidiarias, proveedores de servicios auxiliares, empresas subcontratadas y su personal de resguardar la confidencialidad de los datos que se recaben en el curso de sus actividades[83/]; el Reglamento de Personas Refugiadas, que establece el principio de confidencialidad referente al registro y tratamiento de la información de las personas en condición de refugiadas[84/]; el Reglamento de Acceso Universal, que extiende el régimen de protección reconocido en la Ley General de Telecomunicaciones a los beneficiarios del Fondo Nacional de Telecomunicaciones[85/]; la Política Judicial dirigida al Mejoramiento del Acceso a la Justicia de las Niñas, Niños, y Adolescentes, que incluye disposiciones para salvaguardar el derecho de estos individuos a la dignidad y a la privacidad/protección de datos[86/], y la Directriz para reducir la Revictimización de Niños, Niñas y Adolescentes en Condición de Discapacidad en Procesos Judiciales, que ordena a las autoridades judiciales proteger la privacidad de las personas en situación de vulnerabilidad dentro de un proceso judicial.[87/]

Además, Costa Rica también ha firmado tratados internacionales relacionados con diversos temas que dieron lugar a la aprobación de leyes de tipo sectorial con reglas referentes a la privacidad/protección de datos. A manera de ejemplo cabe mencionar el Protocolo Facultativo de la

---

81. Ley General de Telecomunicaciones N.º 8642, 4 de junio de 2008, *artículos 42 y 43.*
82. Reglamento sobre Medidas de Protección de la Privacidad en las Comunicaciones, Decreto Ejecutivo N.º 35205, 16 de abril de 2009.
83. Ley Reguladora del Contrato de Seguros N.º 8956, 17 de junio de 2011, artículo 21.
84. Decreto Ejecutivo N.º 36831, 28 de setiembre de 2011, artículo 8.
85. Reglamento de Acceso Universal, Servicio Universal y Solidaridad, 6 de octubre de 2008, *artículo 28.*
86. Norma del Poder Judicial, en la Circular N.º 63, 31 de mayo de 2011.
87. Circular 168, 7 de diciembre de 2010.

Convención sobre los Derechos del Niño Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de Niños en la Pornografía, en el que se establece la obligación de los Estados de proteger la intimidad e identidad de los niños que son víctimas de estos delitos, en todas las etapas de los procedimientos penales[88/]; el Acuerdo con el Gobierno de Francia sobre Readmisión de Personas en Situación Irregular, en el que se establece que los datos personales de una persona readmitida han de ser tratados y protegidos conforme a la legislación correspondiente, vigente en cada Estado[89/], y la Convención Internacional para la Protección de Todas las Personas contra las Desapariciones Forzadas, en el que se establece que una persona que se encuentre bajo custodia judicial tiene derecho a que su intimidad/datos estén protegidos cuando su divulgación puede representar un daño para ella misma, entre otros.[90/]

Costa Rica es también signatario de las Reglas Mínimas para la Difusión de Información Judicial en Internet, conocidas como "Reglas de Heredia", que fueron aprobadas en el Seminario Internet y Sistema Judicial realizado en la ciudad de Heredia (Costa Rica), los días 8 y 9 de julio de 2003, con la participación de poderes judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay. Se trata de una serie de diez recomendaciones y cinco alcances, más una serie de definiciones, con los que se pretende ayudar a los sistemas judiciales de los países signatarios a adoptar políticas para la difusión y publicación en Internet de los asuntos que se ventilan en los tribunales y los fallos correspondientes. Estas reglas promueven una mayor difusión de la información, pero requieren que se haga conforme a los principios de autodeterminación informativa y la privacidad/protección de datos.

Por último, cabe hacer notar también que en las leyes de Costa Rica se define lo que constituye un documento privado. En este sentido, se ha aprobado la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, derivada directamente del artículo 24 constitucional, en el cual se establecen los que deben considerarse documentos privados: la correspondencia epistolar, por fax, télex, telemática o cualquier otro medio; los videos, los casetes, las cintas magnetofónicas, los discos, los disquetes, los escritos, los libros, los memoriales, los registros, los planos, los dibujos, los cuadros, las radiografías, las fotografías y cualquier otra forma de registrar información de carácter privado, utilizados con carácter representativo o declarativo, para ilustrar o comprobar algo.[91/]

iii. Habeas data

Según se indicó anteriormente, las leyes de Costa Rica contemplan un procedimiento regulado que corresponde al proceso conocido como habeas data, que permite a los ciudadanos conocer los datos referentes a su persona almacenados en cualquier base de datos. Las leyes antes mencionadas garantizan los derechos conferidos a los individuos cuyos derechos y privilegios

88. Protocolo Facultativo de la Convención sobre los Derechos del Niño Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de Niños en la Pornografía, aprobado mediante la Ley N.º 8172, 7 de diciembre de 2001, artículo 8.
89. Ley N.º 7993, 7 de marzo de 2000, articulo 8.
90. Ley N.º 9005, 31 de octubre de 2011, artículo 20.
91. Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones N.º 7425, 9 de agosto de 1994.

referentes a la autodeterminación informativa han sido violados y les permiten conocer, rectificar o eliminar dicha información.[92/]

iv. Autoregulación

Los códigos de conducta (ética profesional) son relativamente comunes en los diferentes gremios profesionales y pretenden una autoregulación en ciertos temas de su competencia. No obstante, en materia de autodeterminación informativa no existen códigos de conducta que incidan directamente en la privacidad/protección de datos. Quizás el único intento por garantizar la privacidad/protección de datos en el sector privado –sin tratarse específicamente de la autodeterminación informativa– es el caso del Colegio de Periodistas de Costa Rica que emitió un Código de Ética en el que se establece que los periodistas están obligados a conducirse de manera respetuosa en la obtención de información con respeto al dolor ajeno, la privacidad y la intimidad[93/], y a respetar el derecho a la privacidad de las personas físicas y jurídicas socialmente vulnerables.[94/]

No existe un código similar para otros gremios de profesionistas en materia de privacidad/protección de datos o con el que se pretenda garantizar el respeto de la autodeterminación informativa. Sin embargo, el sector privado debe ajustar sus acciones a las normas de derecho positivo mencionadas anteriormente.

B. Ejecución

i. Mecanismo de ejecución

La nueva ley requiere el establecimiento de un procedimiento de ejecución y la creación de la Agencia de Protección de Datos de los Habitantes (Prodhab). Aunque esta entidad está todavía en etapa de planificación, se pretende que funcione bajo el principio de denuncia conforme al cual se requiere que la persona que considere que se han violado sus derechos a la privacidad/protección de datos de cualquier forma, por obra de actores del sector público o privado, para hacer uso de este recurso.[95/] Al recibir una denuncia, se conferirá al responsable de la base de datos un plazo de tres días hábiles para que se pronuncie acerca de la veracidad de los cargos que se le imputen y para que presente pruebas en su defensa. En caso en que la parte acusada no se pronuncie dentro del plazo establecido, la denuncia será considerada debidamente fundada.[96/]

En cualquier momento, la Prodhab podría ordenar al responsable de la base de datos que proporcione cualquier información necesaria e incluso puede realizar inspecciones directamente en el lugar en el que se encuentren los archivos o bases de datos. Además, Prodhab también puede dictar medidas cautelares que lleven a buen término el proceso y para salvaguardar los derechos de las personas. Prodhab deberá emitir su fallo final en el plazo de un mes contado a partir de la presentación de la denuncia. Las resoluciones de la Prodhab podrán ser apeladas en un plazo de tres días después de haber sido emitidas y deberán ser resueltas en el término de ocho días después de presentada la apelación correspondiente.

---

92. Ley N.º 8968 , 7 de julio de 2011, artículo 7.
93. Reglamento N.º 158 , 16 de agosto de 2011, párrafo 24.
94. Artículo 38.
95. Artículo 24.
96. Artículo 25.

En caso de que la Prodhab determine que la información del interesado objeto de la denuncia es falsa, incompleta, inexacta o bien que, de acuerdo con las normas sobre protección de datos personales, fue indebidamente recolectada, almacenada o difundida, deberá ordenarse su inmediata supresión, rectificación, adición o aclaración, o bien impedimento respecto de su transferencia o difusión. Si la persona obligada a cumplir con la resolución de la Prodhab no cumple íntegramente lo ordenado, estará sujeta a las sanciones previstas en la ley de protección de datos y otras leyes.[97/]

Prodhab puede también, ex oficio o a instancia de parte, iniciar un procedimiento tendiente a demostrar si una base de datos regulada por la ley de protección de datos está siendo empleada de conformidad con sus principios. Puede asimismo emitir resoluciones de carácter vinculante[98/], que podrán ser objeto de apelación en un plazo de tres días.[99/] Temporalmente, mientras la Prodhab no entre en funcionamiento pleno, el canal por el que un ciudadano puede proteger sus datos personales debe ser mediante la interposición de un recurso de amparo ante la Sala Constitucional, órgano que ha tenido jurisdicción para resolver asuntos relativos a la privacidad/protección de datos.[100/]

ii. Protección de datos/autoridades ejecutoras

La Ley N.º 8968 dispone la creación de la Prodhab, que estará adscrita al Ministerio de Justicia y Paz como entidad descentralizada con plenas facultades jurídicas y operativas para llevar a cabo los deberes que se le asigne y para manejar sus propios recursos y presupuesto. La Prodhab estará facultada para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones, y además tendrá independencia de criterio.[101/]

Todavía no se han asignado los recursos humanos a la Prodhab pero se prevé que cuente con el personal técnico y administrativo necesario para el adecuado desempeño de sus funciones. El personal será seleccionado por concurso conforme al Estatuto de Servicio Civil o según se dispongan en el reglamento de la ley, que aún falta por emitir.[102/]

Luego de la aprobación de la ley, el 22 de noviembre de 2011 se suscribió el Acuerdo N.º 212 en el que se declara que la creación de la Prodhab es de interés público y nacional. El texto de este acuerdo indica que, para la puesta en marcha de la Prodhab, se conformará una comisión que se encargará de coordinar, planificar y definir todos los aspectos necesarios para la debida implementación de la referida agencia. Esta comisión estará conformada por la Directora Jurídica del Ministerio de Justicia y Paz, quien ejercerá las funciones de coordinación, la Directora Jurídica del Registro Nacional, un representante del Despacho del Ministro de Justicia y Paz, un representante de la Dirección de Apoyo al Consumidor, un representante del Ministerio de Ciencia y Tecnología, un representante del Ministerio de Comercio Exterior, un representante de la Procuraduría de la Ética

---

97. Artículo 26.
98. Las auditorías de bases de datos serán reguladas conforme a la Ley General de la Administración Pública.
99. Previo a la normalización de los procedimientos de la nueva ley de protección de datos, en todo lo no previsto expresamente por la ley de marras serán aplicables las disposiciones del Libro II de la Ley General de la Administración Pública N.º 6227 del 2 de mayo de 1978.
100. Ley sobre Protección de Datos, artículo 29, y Ley de la Jurisdicción Constitucional N.º 7135, 11 de octubre de 1989.
101. Ley N.º 8968, artículo 15.
102. Artículo 18

Pública, así como un representante de la Defensoría de los Habitantes de la República en calidad de observador.

Además, la comisión encargada de la creación de la Prodhab será responsable de redactar el reglamento de la Ley de Protección de Datos Personales, que deberá estar finalizado en un plazo máximo de 6 meses, contados a partir de la puesta en marcha de la agencia. Cabe hacer notar también que las dependencias e instituciones de los sectores público y privado podrán contribuir a la creación de la Prodhab, en la medida de sus posibilidades y dentro del marco jurídico respectivo.

A la fecha, la Prodhab aún no cuenta con un presupuesto, pero este tema está contemplado en la legislación y será fijado de acuerdo con las circunstancias de cada uno de sus componentes.[103/] Además del control apropiado en la asignación de recursos, la Prodhab estará sujeta al cumplimiento de los principios sobre Administración Financiera de la República y Presupuestos Públicos, y estará obligada a proporcionar la información que le requiera el Ministerio de Finanzas.[104/] Además, la Prodhab estará sujeta solamente a las disposiciones de la Contraloría General de la República.

A la fecha, la Sala Constitucional se ha encargado de resolver los casos relativos a la privacidad/datos personales. Según las estadísticas del Sistema Costarricense de Información Jurídica (SCIJ), la Sala Constitucional ha recibido 1396 casos de violación de la intimidad y 266 casos de violación de la protección de datos.

iii. Recursos

Cualquier persona que considere que sus derechos han sido afectados al ser procesados sus datos personales debe solicitar formalmente al procesador de los datos que retire, actualice o bloquee la información en cuestión, o solicitar que no sean utilizados para propósitos distintos de aquellos para los que fueron recopilados, conforme a los principios de la autodeterminación informativa contenidos en la ley de protección de datos. La persona afectada debe seguir este procedimiento antes de recurrir al procedimiento de amparo para proteger sus derechos.

La persona cuyos derechos a la privacidad/protección de datos han sido afectados puede llevar su caso ante las instancias jurídicas pertinentes, conforme al derecho civil, penal o administrativo. Para los casos de responsabilidad civil, lo que incluye a cualquier compañía que procese datos personales, y en una situación no resuelta por la Prodhab, la persona puede entablar una demanda por infracción a las normas civiles, estableciendo los daños que haya sufrido. Cabe destacar que la interposición de una demanda por un caso de responsabilidad civil como el mencionado anteriormente no es obstáculo para presentar, en paralelo o con posterioridad, una apelación conforme a las leyes costarricenses para proteger además los derechos fundamentales de la persona.

Asimismo, si un procesador de datos no responde a una petición o si el interesado no queda satisfecho con la respuesta, puede acudir directamente a la Sala Constitucional para interponer un recurso de amparo. La persona puede también acogerse a este recurso para solicitar que el procesador de datos actualice, corrija, bloquee o retire sus datos personales.

---

103. Ley N.º 8968, artículo 20.

104. Ley N.º 8131, títulos II y X, 8 de septiembre de 2001.

iv. Capacidades de investigación/procesamiento penal

Según se indicó anteriormente, la ley de protección de datos permite a la Prodhab actuar de oficio o a petición de una de las partes. Por lo general, en los casos en los que la Prodhab ve un indicio de violación de los derechos de privacidad/protección de datos de la persona, puede iniciar una investigación para determinar si los datos que posee el procesador están siendo manejados conforme a los principios y requerimientos que marca la ley. Además, cuando sea procedente y no contravenga la ley de protección de datos, procederán también las disposiciones de la Ley General de la Administración Pública. Las apelaciones a los fallos de la Prodhab deberán ser presentadas en un plazo de tres días.[105/]

Según las leyes de Costa Rica, el uso inadecuado de datos íntimos o privados es considerado un delito. El Código Penal dispone pena de prisión de seis meses hasta dos años para aquella persona que atente contra la privacidad de otra o que sin su consentimiento se apodere, accese, modifique, altere, borre, intercepte, interfiera, utilice, difunda o desvíe información de su destino, o que grabe datos e imágenes en medios electrónicos, computadoras, medios magnéticos o telemáticos La pena por actos cometidos por personas encargadas de soportes electrónicos, computadoras, magnéticos y telemáticos irá de uno a tres años.[106/]

La fiscalía se encarga de tramitar las denuncias por violación a las comunicaciones de los ciudadanos, siempre y cuando se cumplan los requisitos del tipo penal, esto es, la intención del sujeto activo de vulnerar la intimidad de la víctima o descubrir sus secretos, o bien, que la acción se realice sin la autorización de la persona.

Desde 2001 cuando se instauró la sanción penal, se han reportado 169 casos de supuestas violaciones de las comunicaciones electrónicas, según consta en el siguiente cuadro:

	2001	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**TOTAL**
Violación de las comunicaciones electrónicas	0	0	0	7	5	11	21	32	51	42	169

C. Cooperación transfronteriza

i. Transferencia de datos

Según la ley de protección de datos, la regla general es que los responsables de las bases de datos (públicas o privadas) solo podrán transferir datos cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos

105. Ley N.º 8968, artículo 27.
106. Código Penal N.º 4573 , 4 de mayo de 1970, artículo 196 bis.

en esta ley. De esta forma, quedan amparadas tanto las transferencias internas como las hechas a otros países.[107/]

ii. Instrumentos/acuerdos internacionales

Costa Rica no forma parte de ningún instrumento o acuerdo internacional de cooperación transfronteriza en materia de privacidad/acceso a la información. Sin embargo, es miembro de la RIPD y es signatario del Declaración de La Antigua Guatemala, en la que se establecen directrices voluntarias sobre privacidad/protección de datos. Asimismo, participó en la XIII Cumbre Iberoamericana de 2003 en la que los Jefes de Estado declararon ser conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacaron la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos de la región. En otros foros internacionales, tales como el Diálogo Político y Cooperación entre la Comunidad Europea y sus Estados Miembros y las repúblicas de Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá, de 2010, Costa Rica ha cooperado con otros Estados para garantizar la protección de datos personales, mejorar el nivel de protección y promover el libre movimiento transfronterizo.

Colombia no ha solicitado todavía la certificación de la Unión Europea.

iii. Cooperación transfronteriza en materia de investigación y ejecución de las leyes

Como regla general, la legislación de Costa Rica permite el intercambio de información con autoridades en jurisdicciones fuera del territorio nacional, en particular en materia de delincuencia organizada nacional y transnacional, terrorismo, narcotráfico, fraude bancario, etc[108/]. Sin embargo, esto depende del delito en particular. En virtud de que la ley de protección de datos fue promulgada relativamente hace poco tiempo y de que apenas se está estableciendo la Prodhab, parece poco probable que las autoridades, por lo menos en el corto plazo, estén en condiciones de cooperar en cualquier esfuerzo transfronterizo en materia de privacidad/protección de datos. Además, la ley de protección de datos no dispone expresamente la cooperación con gobiernos y entidades encargadas de la protección de datos, ni establece obligación alguna para que la Prodhab coopere con entidades extranjeras encargadas de la ejecución de leyes relativas a esta materia. No obstante, es posible que esta cooperación sea una realidad en el futuro.

D. Jurisprudencia y retos especiales

La jurisprudencia nacional ha permitido a los ciudadanos ejercer sus derechos relacionados con el tratamiento de datos personales. Sin embargo, los tribunales han enfrentado retos muy particulares dada la existencia de un nuevo derecho sin contar con disposiciones legislativas sobre la privacidad/protección de datos. En principio, los casos eran resueltos teniendo como base los conceptos tradicionales de privacidad o intimidad, pero ello dio como resultado una legislación confusa y a veces contradictoria. Poco a poco, los tribunales llegaron a reconocer el derecho a la autodeterminación informativa y la protección de los datos personales, lo cual condujo al

107. Ley N.º 8968, 7 de julio de 2011, artículo 14.

108. Ley contra la Delincuencia Organizada N.º 8754, 22 de julio de 2009, artículo 11.

establecimiento de criterios y una aplicación más uniforme del sistema judicial. Cabe destacar el hecho de que la Sala Constitucional reconoció que el derecho a la autodeterminación informativa tiene como base los siguientes principios: el de transparencia sobre el tipo, dimensión o fines del procesamiento de los datos guardados; el de correspondencia entre los fines y el uso del almacenamiento y empleo de la información; el de exactitud, veracidad, actualidad y plena identificación de los datos guardados; el de prohibición del procesamiento de datos relativos a la esfera íntima del ciudadano (raza, creencias religiosas, afinidad política, preferencias sexuales, entre otras) por parte de entidades no expresamente autorizadas para ello; y de todos modos, el uso que de la información se haga debe ser acorde con lo que con ella se persigue; el de la destrucción de datos personales una vez que haya sido cumplido el fin para el que fue recopilada, entre otros. Otra decisión importante de la Sala Constitucional establece cierta jerarquía para los tipos de datos personales, confiriendo así un mayor nivel de escrutinio y seguridad a los datos confidenciales relativos a las preferencias sexuales, el grupo étnico, las creencias religiosas y la afinidad política, considerados como aspectos inherentes de la personalidad.[109/]

5. República Dominicana

A. Contexto jurídico

i. Marco constitucional

La Constitución de República Dominicana establece los siguientes derechos: derecho a la intimidad y el honor personal[110/], acceso a la información y libertad de expresión[111/] y el recurso de habeas data.[112/]

ii. Marco legislativo

El artículo 44 de la Constitución dispone un derecho más amplio a la intimidad y honor personal al establecer que todas las personas tienen derecho a la intimidad, a la no injerencia en la

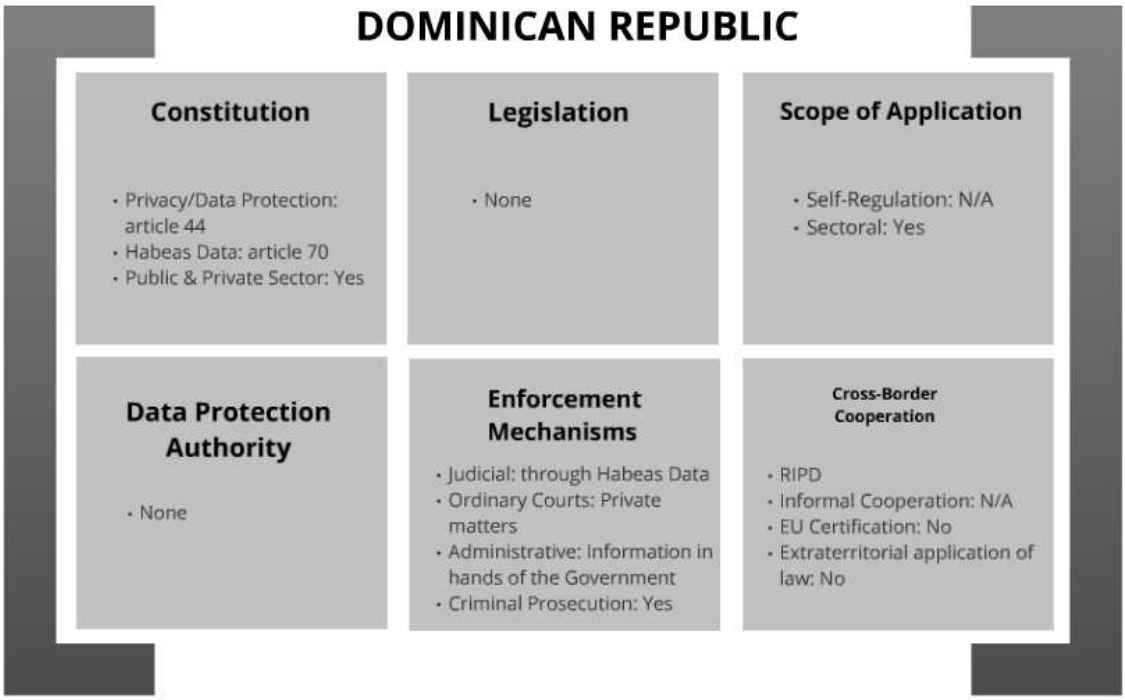
---

109. Un análisis detallado e historia de la jurisprudencia costarricense en materia de privacidad/protección de datos se encuentra en las respuestas de Costa Rica al Cuestionario de Legislación y Prácticas sobre Privacidad y Protección de Datos de la CAJP, documento CP/CAJP-3026/11 add. 6, disponible en: http://www.oas.org/dil/esp/proteccion_de_datos_cuestionario_Costa_Rica.pdf
110. Constitución de la República Dominicana, artículo 44.
111. Artículo 49. Libertad de expresión e información. Toda persona tiene derecho a expresar libremente sus pensamientos, ideas y opiniones, por cualquier medio, sin que pueda establecerse censura previa: 1) Toda persona tiene derecho a la información. Este derecho comprende buscar, investigar, recibir y difundir información de todo tipo, de carácter público, por cualquier medio, canal o vía, conforme determinan la Constitución y la ley; 2) Todos los medios de información tienen libre acceso a las fuentes noticiosas oficiales y privadas de interés público, de conformidad con la ley; 3) El secreto profesional y la cláusula de conciencia del periodista están protegidos por la Constitución y la ley; 4) Toda persona tiene derecho a 1a réplica y rectificación cuando se sienta lesionada por informaciones difundidas. Este derecho se ejercerá de conformidad con la ley; 5) La ley garantiza el acceso equitativo y plural de todos los sectores sociales y políticos a los medios de comunicación propiedad del Estado.
112. Constitución, artículo 70. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquellos, conforme a la ley.

vida privada, la familia, el domicilio y la correspondencia del individuo, así como el derecho al honor, al buen nombre y a la propia imagen. Cualquier autoridad o entidad (pública o privada) que viole este derecho estará obligada a resarcirlos conforme a la ley[113/]. Además, la ley dispone reglas específicas/sectoriales sobre privacidad/protección de datos en los siguientes contextos especializados: el Código Tributario, el Código Procesal Penal, el Código de Protección de Niños, Niñas y Adolescentes, el Código Penal, la Ley General de Libre Acceso a la Información Pública, la Regulación de las sociedades de información crediticia y de protección al titular de la información[114/], la Ley Monetaria y Financiera[115/], la Ley sobre el Síndrome de Inmunodeficiencia Adquirida[116/], la Ley General de Salud[117/], la Ley sobre Telecomunicaciones[118/] y el Reglamento para la autorización de intervenciones telefónicas.[119/]

En la actualidad, un Anteproyecto de Ley de Protección de Datos Personales está siendo analizado por el Poder Ejecutivo antes de ser enviado al Congreso Nacional para su aprobación.

113. Artículo 44 de la Constitución. Establece específicamente que: 1) El hogar, el domicilio y todo recinto privado de la persona son inviolables, salvo en los casos que sean ordenados, de conformidad con la ley, por autoridad judicial competente o en caso de flagrante delito; 2) Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como a conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos; 3) Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Solo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia; 4) El manejo, uso o tratamiento de datos e informaciones de carácter oficial que recaben las autoridades encargadas de la prevención, persecución y castigo del crimen, solo podrán ser tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio, de conformidad con la ley;
114. Ley N.º 288-05.
115. Ley N.º 183-05.
116. Ley N.º 55-93.
117. Ley N.º 42-01.
118. Ley N.º 153-98.
119. Ley N.º 122-07.



iii. Habeas data

La Constitución de República Dominicana prevé el mecanismo de habeas data[120/], el cual figura en la Ley Orgánica del Tribunal Constitucional y de los Procedimientos Constitucionales. Esta figura jurídica puede ser incoada en cualquier tribunal del país bajo el régimen del amparo. El procedimiento específico establece que toda persona tiene derecho a una acción judicial para conocer de la existencia de datos personales, ya sea en bases de datos públicas o privadas, y tener acceso a ellos. En aquellos casos en los que se determine que la información es incorrecta o de naturaleza discriminatoria, la persona puede solicitar la suspensión, rectificación, actualización y confidencialidad de estos.[121/]

iv. Autoregulación

En la actualidad no existen códigos autorregulatorios de la conducta sobre privacidad/protección de datos en República Dominicana.

---

120. El artículo 70 de la Constitución establece que toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquellos.
121. Ley Orgánica del Tribunal Federal y de los Procedimientos Constitucionales, artículo 64. La ley establece además que la acción del habeas data está regida por el sistema procesal de amparo.

B. Ejecución

i. Mecanismos de ejecución

En la actualidad, el único mecanismo para hacer valer los derechos a la privacidad/datos personales es el recurso de habeas data (descrito anteriormente). Por lo que se refiere a las cuestiones de índole privada, estas deben ser llevadas ante los tribunales ordinarios. En cuanto a las cuestiones de información en poder del Estado, se acude ante la jurisdicción administrativa.[122/]

ii. Protección de datos/autoridades ejecutoras

República Dominicana no cuenta con un órgano que se encargue íntegramente del cumplimiento de las leyes relativas a la privacidad/protección de datos. Sin embargo, existen entidades de Gobierno encargadas de supervisar el cumplimiento de algunas leyes y reglamentos locales en la materia. Un ejemplo de ello es la protección de los derechos del consumidor en general (incluido el derecho a la intimidad) que son velados por el Instituto Nacional de Protección de los Derechos del Consumidor (Proconsumidor) y los Juzgados de Paz.[123/] En el caso de datos procesados por las oficinas calificadoras de crédito privadas, el órgano competente es la Superintendencia de Bancos.[124/]

iii. Recursos

Los individuos afectados tienen a su disposición el recurso de habeas data. Asimismo, en el Ministerio Público puede entablar acciones contra actores públicos o privados por violación a los derechos a la intimidad conforme al Código Procesal Penal.

C. Cooperación transfronteriza

i. Transferencia de datos

Las leyes locales no establecen condición alguna para el flujo transfronterizo de datos.

ii. Instrumentos/acuerdos internacionales

República Dominicana ha participado en la RIPD pero no forma parte de ningún acuerdo o convenio formal sobre cooperación transfronteriza.

iii. Cooperación transfronteriza en materia de investigación y ejecución de las leyes

El Código Procesal Penal permite el intercambio de información con autoridades y tribunales en otros países en aquellos casos en los que exista una investigación en proceso.

---

122. Ley N.º 13-07.
123. Constitución y Ley N.º 358-05.
124. Ley N.º 288-05.

D. Jurisprudencia y retos especiales

Según la información proporcionada por República Dominicana en sus respuestas al Cuestionario de Protección de Datos, los tribunales locales solo han recibido un caso sobre protección de la privacidad/protección de datos.

6. El Salvador

A. Contexto jurídico

i. Marco constitucional

La Constitución de El Salvador no contempla ninguna regulación explícita sobre la protección de la privacidad/protección de datos. Sin embargo, el artículo 2 de la Constitución garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Ello implica que el derecho a la autodeterminación informativa es un derecho fundamental implícitamente incorporado en la Constitución.[125/] Aunque los derechos a la privacidad/protección de datos no están contemplados expresamente en la Constitución, pueden encajar perfectamente en el artículo 2 en virtud de que están estrechamente vinculados al derecho a la intimidad personal y familiar y a la propia imagen, de tal manera que su tutela no quedaría excluida de otros derechos reconocidos por la Constitución.

Asimismo, la Constitución hace referencia expresa a la libertad de expresión en su artículo 6, el cual establece que: "Toda persona puede expresar y difundir libremente sus pensamientos siempre que no subvierta el orden público, ni lesione la moral, el honor, ni la vida privada de los demás".

El recurso de habeas data no está incluido en la Constitución de El Salvador.

ii. Marco legislativo

De igual modo, El Salvador no cuenta con una ley relativa a la privacidad/protección de datos. Sin embargo, el marco jurídico local cuenta con diversas leyes referentes a aspectos esenciales de la privacidad/protección de datos. Otras legislaciones secundarias han incorporado disposiciones relativas a la privacidad/protección de datos, la mayoría de las cuales pueden aplicarse por igual tanto al sector público como al privado.

Entre estas normas se encuentran las siguientes: el Código Penal que regula los delitos relativos al honor y la intimidad (arts. del 177 al 190)[126/]; el Código Procesal Penal; Ley de Ética Gubernamental; la Ley de Protección al Consumidor[127/]; la Ley de Bancos, principalmente en lo

---

125. Se entiende que el derecho a la protección de datos y a la privacidad está contenido implícitamente en el artículo 2 de la Constitución, que establece que toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa del honor, de la intimidad personal y familiar y a la propia imagen.
126. Código Penal, artículos del 177 al 190.
127. Ley de Protección al Consumidor, artículo 49.

referente al secreto bancario[128]; la Ley contra el Lavado de Dinero y Activos[129]; la Ley Especial para la Protección de Víctimas y Testigos; el Convenio Centroamericano para la Protección de Víctimas, Testigos, Peritos y demás Sujetos que Intervienen en la Investigación y en el Proceso Penal, particularmente en el narcotráfico y la delincuencia organizada; la Ley de Adquisiciones y Contrataciones de la Administración Pública; la Ley de Acceso a la Información Pública (ya en vigencia pero en proceso de implementación), que prohíbe proporcionar información o registros de carácter personal por considerarla confidencial[130]; la Ley Penal Juvenil, que reconoce el derecho a la intimidad personal de los menores y regula la confidencialidad del Libro de Registro de Internamiento[131]; la Ley de Protección Integral de la Niñez y Adolescencia, que reconoce el derecho al honor, la imagen, la vida privada y la intimidad, entre otros.[132]

iii. Habeas data

La figura del habeas data no está contemplada en el sistema jurídico de El Salvador, pero ello no implica que este derecho no esté protegido. Este derecho queda implícito en el artículo 2 de la Constitución, como ya se mencionó, y el artículo 247 establece además que: "toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia por violación de los derechos que otorga la presente Constitución", de donde se infiere que, tanto los derechos

128. Ley de Bancos, artículo 232.
129. Ley contra el Lavado de Dinero y Activos, artículos 24 y 25.
130. Ley de Acceso a la Información Pública, artículos 24, y del 31 al 44.
131. Ley Penal Juvenil, artículo 2, 122 y 123.
132. Ley de Protección Integral de la Niñez y Adolescencia, artículo 46.

reconocidos expresamente como los contenidos implícitamente deben ser garantizados a toda persona a través de los mecanismos de protección establecidos para su ejercicio.

iv. Autoregulación

En El Salvador no existen regulaciones específicas sobre la privacidad/protección de datos. En consecuencia, no existen códigos de autocontrol ni otros sistemas similares de autorregulación para la protección de estos derechos. En cualquier caso, existen algunos reglamentos en el sistema jurídico de El Salvador relacionados con la materia, como es el caso del Código de Ética Periodística.

B. Ejecución

i. Mecanismos de ejecución

La constitución de El Salvador establece que "toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia por violación de los derechos que otorga la presente Constitución", lo cual incluye los derechos implícitos y explícitos conferidos a toda persona a través de los mecanismos de protección establecidos.[133/] Así pues, ante la falta de una legislación específica puede entenderse que la privacidad/protección de datos pueden ser garantizados a través del proceso constitucional de amparo.

En el ámbito penal, el honor y la intimidad son entendidos como bienes jurídicos merecedores de protección, por lo cual, se han tipificado como delito un conjunto de conductas que suponen una lesión grave a estos bienes. Por ejemplo, el Código Procesal indica que este tipo de delitos son perseguibles por acción privada, es decir, únicamente por acusación de la víctima.[134/] Además, estas normas regulan un procedimiento especial (y más expedito) que puede utilizarse en estos casos.[135/]

ii. Protección de datos/autoridades ejecutoras

En virtud de que en El Salvador no existen leyes referentes a la protección de datos, ello implica que tampoco existe una autoridad en la materia. En consecuencia, las autoridades cuya responsabilidad principal es hacer valer las leyes vigentes relacionadas con la privacidad/protección de datos son los jueces de la Sala de lo Constitucional de la Corte Suprema de Justicia, quienes pueden escuchar algunos casos específicos presentados por vía del amparo.

iii. Recursos

Tal como se indicó anteriormente, el recurso por excelencia para la persona cuyos derechos de privacidad/protección de datos han sido violados es el recurso de amparo, aunque también existe en el Código Procesal.

---

133. Constitución, art. 247.
134. Código Procesal, artículo 28.
135. Código Procesal, artículos del 439 al 444. Un proceso expedito para la defensa de los derechos de privacidad incluye: a) presentación del escrito de acusación a un tribunal de sentencia; b) intimación del inculpado; c) conciliación; d) audiencia de aportación y admisión de pruebas, y e) sentencia.

iv. Capacidades de investigación

Las autoridades no tienen las facultades para realizar investigaciones, excepto en la proposición de pruebas de casos llevados ante el poder judicial.

C. Cooperación transfronteriza

El Salvador no forma parte de ningún convenio internacional sobre privacidad/protección de datos. El actual marco jurídico no regula ni prohíbe la transferencia de datos. La cooperación internacional es posible conforme a los procesos de cooperación internacionales en materia penal y conforme las leyes locales.

7. México

Las respuestas de México al Cuestionario de Legislación y Prácticas sobre Privacidad y Protección de Datos de la CAJP se encuentran en el documento CP/CAJP-3026/11 add. 7, al que se adjunta la nota OEA-00265, fechada el 8 de febrero de 2012, y que constituye la base para la información que se resume en esta sección.

A. Contexto jurídico

i. Marco constitucional

La Constitución Política de los Estados Unidos Mexicanos contiene varias disposiciones relacionadas con la privacidad/protección de datos. El artículo 6 alude a la libertad de expresión, acceso a la información y protección de datos, al señalar que la manifestación de las ideas no puede ser objeto de ninguna inquisición judicial o administrativa, excepto si va en contra de la moral, los derechos de terceros, provoca algún delito o perturba el orden público. Asimismo, indica que el derecho a la información tiene que ser garantizado por el Estado y que la Federación y los gobiernos de los Estados deben proteger la información que se refiere a la vida privada y a los datos personales, en los términos y con las excepciones que dispone la ley.

El artículo 7 trata sobre la libertad de expresión, garantiza la libertad de prensa y garantiza también que ninguna autoridad gubernamental puede censurar ni violar la libertad de escribir y publicar escritos sobre cualquier materia. La única limitación a este derecho tiene que ver con el respeto a la vida privada del individuo, a la moral y a la paz pública.

El artículo 6 dispone asimismo el derecho al habeas data y el derecho al libre acceso a los datos personales en poder de entidades públicas, y rectificarlos/corregirlos en caso de que sean incorrectos. El artículo 16 hace referencia a la protección de datos ya que establece que toda persona tiene derecho a la protección de sus datos personales, a su acceso, rectificación y cancelación, así como a manifestar su oposición, en los términos que señale la ley, la cual debe fijar los supuestos de excepción a los principios que rijan el tratamiento de datos por motivos de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

El artículo 20 establece el derecho a retener o conocer los datos personales de las personas en su defensa en un proceso penal, y el artículo 73 (sección XXIX-O) otorga al Congreso de la Unión el poder de legislar sobre los datos personales en posesión de individuos/entidades.

ii. Marco legislativo

En el ámbito nacional, la legislación sobre privacidad/protección de datos abarca los sectores público y privado. La legislación federal sobre transparencia/acceso a la información regula la protección de datos cuando se trata de información procesada o custodiada por entidades del Gobierno federal. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) regula la privacidad/protección de datos procesados o custodiados por individuos/entidades en el ámbito nacional. En el ámbito estatal, los 31 estados (y el Distrito Federal) han promulgado leyes sobre transparencia/acceso a la información, que también regulan la protección de datos procesados o custodiados por entidades de los Gobiernos de los estados. Las leyes estatales no se aplican al sector privado, el cual está regulado por la LFPDPPP.

Sector público: En el ámbito nacional, entre los instrumentos normativos sobre privacidad/protección en el sector público se incluyen los siguientes: 1) Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) ; 2) Reglamento de la Ley Federal de Transparencia, y 3) Lineamientos de Protección de Datos Personales.

La LFTAIPG y su Reglamento establecen un marco para la protección de datos personales en posesión de autoridades públicas (entidades reguladas). Esta normativa establece los principios fundamentales para el procesamiento, recolección y uso de datos personales, requiere el

consentimiento de la persona cuyos datos son recopilados o procesados (con excepciones) y establece que la recopilación y procesamiento deben ser para un propósito específico. La ley crea el derecho a conocer y corregir la información, define los deberes de confidencialidad y seguridad y establece una autoridad federal independiente para garantizar su cumplimiento.[136/]

El Reglamento de la LFTAIPG establece el procedimiento mediante el cual los individuos pueden solicitar consultar su información personal en todas las entidades federales y solicitar su modificación si los datos están incompletos o incorrectos. El reglamento también establece un procedimiento de apelación ante el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) para aquellos casos en los que la persona no quede satisfecha con la solución dada al problema por las entidades federales.[137/]

Los Lineamientos de Protección de Datos Personales establecen políticas y procedimientos vinculantes para las entidades del Servicio Civil Federal a fin de garantizar que los individuos tienen derecho a decidir sobre el uso y destino de sus datos personales, garantizar que sean procesados y manejados adecuadamente y evitar su transmisión ilícita o lesiva[138/] Estos lineamientos establecen asimismo los principios que regulan el procesamiento de datos personales por parte de la administración pública federal y establecen condiciones y requerimientos mínimos para su manejo y custodia.

En el ámbito estatal, los 31 estados (y el Distrito Federal) han promulgado leyes sobre transparencia/acceso a la información que también regulan la protección de datos procesados o custodiados por entidades de los Gobiernos de los estados. En el cuadro ___ se presenta una lista de las leyes estatales aplicables sobre transparencia/acceso a la información.

Sector privado: En el ámbito nacional, la normativa que rige la privacidad/protección de datos en el sector privado es la LFPDPPP mencionada anteriormente y su reglamento.

Esta ley, publicada el 5 de julio de 2010, tiene como objetivo proteger los datos personales a fin de garantizar que son procesados para propósitos legítimos, con el debido consentimiento informado, así como garantizar el derecho a la privacidad y a la autodeterminación de los individuos. Se aplica a todas las personas (individuos y personas jurídicas) que recopilan, obtienen, procesan, utilizan, difunden o almacenan información personal.[139/] Quedan excluidas las oficinas calificadoras de crédito y las personas que recopilan información para propósitos meramente personales o internos.[140/]

El Reglamento de la LFPDPPP establece el marco para la aplicación efectiva de la ley, incluido el ámbito territorial de aplicación; la fuente de acceso público; las características del consentimiento; el procedimiento para la autorización de medidas compensatorias; los deberes y

---

136. Ley Federal de Transparencia y Acceso a la Información Pública, Título I, Capítulo IV ("Protección de datos personales") y Título II, Capítulo IV ("Del procedimiento ante el IFAI").
137. Capítulos VI ("Información confidencial"), VIII ("Protección de datos personales") y XII ("Del procedimiento de acceso a la información", con algunas disposiciones aplicables al acceso y rectificación de datos).
138. Lineamientos de Protección de Datos Personales, lineamiento primero.
139. Artículo 1 de la LFPDPPP.
140. Artículos 2 y 3, fracción XVIII de la LFPDPPP.

obligaciones específicas del procesador de datos y subcontratistas/terceros; la autorregulación vinculante; el procedimiento de verificación, y el procedimiento de protección de derechos de los individuos. Como se ha indicado, la LFPDPPP se aplica a todo el sector privado del país.

iii. Habeas data

Como se indicó en la subsección (i) anterior, el artículo 16 de la Constitución establece el derecho a acceder a la información personal, así como a su rectificación o cancelación y a manifestar su oposición a que se utilice o procese (derechos ARCO). Estos derechos quedan descritos en leyes específicas para las personas/entidades de los sectores público y privado que procesan o recopilan datos personales.

La LFTAIPG y su reglamento establecen el proceso específico para tener acceso y corregir los datos personales custodiados o en posesión de una entidad federal.

Cada estado del país cuenta con su propio instrumento legal que garantiza el derecho de acceso a los datos personales en posesión de entidades públicas del estado en cuestión.

La LFPDPPP es la que regula el acceso a los datos personales en posesión de entidades privadas (individuos o entidades jurídicas). En contraste con este sistema dividido para el acceso a los datos personales en posesión del sector público, la LFPDPPP regula el acceso a los datos personales custodiados por el sector privado tanto en el ámbito federal como estatal. En particular, la LFPDPPP garantiza que la persona tiene derecho a conocer sus datos personales, a rectificarlos, cancelarlos y oponerse a su procesamiento. El artículo 22 de la LFPDPPP establece que:

Cualquier titular [...] podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

El artículo 23 de la LFPDPPP dispone que los titulares tienen derecho a conocer sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que estén sujetos los datos. El artículo 24 señala que el titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos. El artículo 25 establece que el titular tendrá en todo momento el derecho a cancelar (borrar) sus datos personales. El artículo 27 establece que el titular tendrá derecho, en todo momento y por causa legítima, a oponerse al tratamiento de sus datos.

iv. Autoregulación

La LFPDPPP prevé que los individuos y las entidades tienen derecho a convenir entre ellos las condiciones para el procesamiento de datos personales, dando lugar así a la creación de esquemas autorregulatorios vinculantes[141/], los cuales deben ser registrados ante el IFAI para que tengan validez.[142/]

---

141. LFPDPPP, artículo 44.
142. Reglamento de la LFPDPPP, artículo 86.

A marzo de 2012 no se había inscrito todavía ningún esquema autorregulatorio ante el IFAI. Ello no ha obstado para que algunas compañías privadas cuenten con esquemas autorregulatorios con disposiciones en materia de privacidad/protección de datos. A manera de ejemplo pueden mencionarse las siguientes tres compañías:

La Asociación Mexicana de Internet (AMIPCI), institución privada que integra a empresas de la industria de Internet en México, otorga un sello electrónico de confianza que reconoce a los negocios o instituciones que promueven el cumplimiento de la privacidad de la información. Las compañías que reciban el sello se comprometen a cumplir la normativa de privacidad y el Código de Ética de la AMIPCI.[143/] Se requiere cumplir las normas mínimas, incluida la creación de una política de privacidad, avisos de divulgación, opciones y consentimiento, calidad de los datos y limitaciones de uso y seguridad. El Código de Ética prevé sanciones para cualquier miembro de la asociación que no cumpla esta normativa.[144/]

El Grupo Financiero BBVA ha adoptado un código de ética que incluye disposiciones en materia de privacidad/protección de datos para todas sus instituciones afiliadas, con reglas y procedimientos específicos para proteger y garantizar el procesamiento adecuado de la información de carácter personal recopilada en el transcurso de sus operaciones comerciales y que esté relacionada con sus clientes, accionistas, empleados y gerentes o cualquier otra persona con quien establezcan contacto. Este código dispone, entre otras, las siguientes responsabilidades para la institución y sus empleados: conocer y observar las normas y procedimientos internos en materia de seguridad de la información y de protección de datos de carácter personal; aplicar medidas adecuadas para evitar el acceso indebido a tal información; los empleados que, por razón de su cargo o de su actividad, tengan acceso a datos personales son responsables de su custodia y apropiado uso.

El Grupo Novartis, integrado por empresas farmacéuticas, también ha creado un código de conducta en el que se incluyen los derechos a la privacidad de sus empleados, pacientes, médicos y otras partes interesadas. Este código establece en que deben notificarse a las personas la recopilación y tratamiento de sus datos personales, de que tal recopilación y tratamiento se llevan a cabo solo para propósitos comerciales legítimos y específicos, y la obligación de proteger tales datos contra accesos no autorizados.

Estos representan solo algunos ejemplos de la autorregulación existente en México, aunque debe aclararse que los esquemas y políticas descritos anteriormente no han sido presentados, registrados ni aprobados por el IFAI y que esta institución no ha participado de ningún modo en la creación ni análisis de estos. En cuanto quede completado el sistema para la presentación de esquemas de autorregulación, el IFAI asesorará a las entidades interesadas en establecer sus esquemas autorregulatorios vinculantes y proporcionará los mecanismos de vigilancia para garantizar su cumplimiento.

---

143. En particular, el sello de la AMIPCI promueve el cumplimiento de la LFPDPPP y su Reglamento, la Ley Federal de Protección al Consumidor, el Código de Ética de la asociación y el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico. www.ampici.org.mx. www.sellosdeconfianza.org.mx.
144. Código de Ética de la AMIPCI, artículo 22.

B. Ejecución

i. Mecanismos de ejecución

Los mecanismos de ejecución en México pueden ser voluntarios u obligatorios. En cuanto a los mecanismos voluntarios, la LFPDPPP permite a las partes convenir entre ellas (o con entidades civiles y gubernamentales, nacionales o extranjeras) esquemas de autorregulación vinculantes, como pueden ser códigos deontológicos, prácticas óptimas profesionales, marcas o sellos de confianza, políticas de privacidad, reglas de privacidad corporativa o cualquier otro instrumento que sea registrado ante el IFAI y cualquier otra autoridad sectorial competente.[145/]

Las normas/contenido mínimo de estos esquemas autorregulatorios quedan definidos en la LFPDPPP incluyen los siguientes: ámbito de aplicación; procedimientos que se utilizarán para medir el cumplimiento con las obligaciones relativas a la protección de datos personales; sistemas de supervisión y vigilancia internos y externos; programas de capacitación para las personas que traten los datos; mecanismos que permitan facilitar los derechos de los titulares; identificación de los titulares y personas que entran en contacto con los datos procesados, y medidas correctivas en caso de incumplimiento.[146/]

Estos esquemas de autorregulación incluyen la certificación de los responsables de la protección de datos personales, la cual puede ser otorgada conforme a un procedimiento llevado a cabo por una persona/entidad acreditada que avale que las políticas, programas y procedimientos de privacidad que implementaron las partes aseguran el debido tratamiento de los datos personales y que las medidas de seguridad que adoptaron son las adecuadas para protegerlos.[147/] Asimismo, la LFPDPPP dispone otros mecanismos no coercitivos a cargo del IFAI, que incluyen el ayudar a otras instituciones en la elaboración de sus reglamentos, opiniones y recomendaciones, la divulgación de normas y mejores prácticas internacionales, la cooperación con autoridades supervisoras nacionales e internacionales, la realización de estudios e investigaciones y el ofrecer capacitación a las entidades obligadas.[148/]

En cuanto a los mecanismos coercitivos, la LFPDPPP y su Reglamento establecen procedimientos vinculantes para ejercer los derechos de acceso, rectificación, cancelación y eliminación de datos personales; procedimientos para proteger los derechos de los individuos cuyos datos son procesados; procedimientos de verificación del cumplimiento de esta normativa, y el procedimiento para la imposición de sanciones en casos de violación y no cumplimiento.

Por lo que se refiere a datos personales en manos de entidades del Gobierno federal, el acceso y corrección de los datos personales ocurre ante la entidad federal en cuestión mediante la solicitud correspondiente. En caso de que el solicitante no quede satisfecho con la solución del caso, podrá presentar inconformidad ante el IFAI, el cual revisará y dictaminará la solución del problema. Aunque no se ha presentado ningún caso conforme a esta normativa, las resoluciones que emita el IFAI son susceptibles de ser impugnadas ante el Poder Judicial de la Federación mediante juicio de amparo.

---

145. Artículo 44 de la LFPDPPP y 80 del Reglamento de la LFPDPPP.
146. Reglamento de la LFPDPPP, artículo 82.
147. Reglamento de la LFPDPPP, artículos 83 y 84.
148. LFPDPPP, artículo 39.

En lo que hace a los datos personales en posesión de las entidades de gobierno estatales, las leyes estatales disponen una acción administrativa, generalmente en forma de solicitud, para ejercer uno o más de los siguientes derechos: acceso, rectificación, cancelación y oposición; así como otra, también de carácter administrativo, para impugnar las respuestas proporcionadas a los titulares. Este medio de impugnación generalmente es conocido como "recurso", pero dependiendo de la legislación de que se trate puede denominarse queja, recurso de revisión, recurso de reconsideración, procedimiento de inconformidad, etc.

Tanto para el sector público como el privado, existe la vía judicial como último recurso cuando las personas no quedan satisfechas con las resoluciones obtenidas en otras instancias.[149/]

ii. Protección de datos/autoridades ejecutoras

Por lo que se refiere a la privacidad/protección de datos en el contexto del sector privado y las entidades del Gobierno federal, la autoridad correspondiente es el IFAI, el cual es una entidad descentralizada del Gobierno federal, con autonomía operativa, presupuestaria y de decisión, encargada de promover el derecho a la información, decidir sobre las negativas a las solicitudes de acceso a la información y de la protección de datos personales procesados o en custodia de entidades federales.[150/] Además, el IFAI tiene como mandato la promoción y difusión del derecho a la privacidad/protección de datos en la sociedad mexicana y velar el cumplimiento y aplicación de la LFPDPPP.[151/]

Al año 2012, el IFAI contaba con un total de 393 empleados y un presupuesto de $482,382,497 pesos mexicanos.[152/]

Cabe hacer notar que, además del IFAI, las siguientes autoridades federales son responsables de la aplicación de las leyes sobre privacidad/protección de datos: la Cámara de Senadores, la Suprema Corte de Justicia, la Universidad Nacional Autónoma de México, el Banco de México, el Instituto Federal Electoral, el Instituto Nacional de Estadística, Geografía e Informática y la Comisión Nacional de Derechos Humanos.

Con respecto a la privacidad/protección de datos en el contexto de las entidades estatales gubernamentales y el Distrito Federal, cada gobierno tiene su propia autoridad competente, las

---

149. El juicio de amparo como un medio para ejercer el derecho a la protección de los datos personales está previsto en la Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos.

150. Conforme al artículo 33 de la LFTAIPG.

151. LFPDPPP, artículo 38.

152. www.apartados.hacienda.gob.mx/presupuesto/temas/pef/2012/temas/tomos/06/r06_hhe_afpefe.pdf. Las cifras correspondientes al presupuesto y personal comprenden la totalidad de atribuciones del IFAI entre las que se encuentran las relacionadas con el derecho de acceso a la información y el derecho a la privacidad/protección de datos.

cuales se dividen en los siguientes tres grupos: autoridades estatales con autonomía constitucional[153/], autoridades estatales con autonomía jurídica[154/] y autoridades estatales sin autonomía.[155/]

Para el procesamiento de datos personales en manos de particulares, la LFPDPPP prevé dos procedimientos relacionados con la observancia de los principios y derechos en materia de privacidad. Por una parte, en sus artículos 45 y 58, la LFPDPPP establece el procedimiento para la protección de derechos que en todos los casos se inicia a petición del titular o su representante legal, y en los artículos 59 y 60 se dispone el procedimiento de verificación que puede iniciar de oficio o a petición de parte. En el procedimiento de verificación de oficio, el IFAI cuenta con la facultad para iniciarlo cuando presuma fundada y motivadamente la existencia de violaciones a la LFPDPPP.

iii. Recursos

El IFAI es la autoridad administrativa facultada para vigilar la observancia de la LFPDPPP y de la LFTAIPG, por iniciativa/prerrogativa propia, si hay razón para creer que ha ocurrido una violación, así como para responder a las solicitudes de los individuos. Puede oír impugnaciones en casos en los que las autoridades públicas se han negado a entregar o corregir datos personales, así como en casos en los que el solicitante no ha recibido respuesta. En este último caso, el IFAI debe analizar todas las apelaciones que se le presenten, siempre y cuando contengan todos los elementos jurídicos necesarios para su consideración. La revisión es obligatoria, no es voluntaria ni opcional, y se hace caso por caso.

Con respecto a sector privado, el IFAI está facultado para oír casos y para imponer sanciones contra los infractores.[156/] Una segunda instancia de impugnación es el Tribunal Federal de Justicia Fiscal y Administrativa disponible para aquellas personas que desean apelar las resoluciones del IFAI, y una tercera instancia sería el apelar la decisión de este último tribunal por vía del amparo ante el Poder Judicial de la Federación.[157/]

En el caso del sector privado, el IFAI ha recibido un total de 70 quejas contra el sector privado desde que entró en vigor en enero de 2012.[158/]

En cuanto al sector público, el IFAI está facultado para oír y decidir apelaciones en cuanto al acceso a la información y la protección de los datos. Sin embargo, este instituto solo puede notificar a las entidades federales que estén bajo su jurisdicción cuando ha ocurrido una infracción a la ley o a su reglamento; y según la LFTAIPG, no tiene facultad para imponer sanciones a las entidades del sector público. A diferencia de las apelaciones contra el sector privado, cabe hacer notar que las personas solo tienen un recurso contra las resoluciones del IFAI, es decir, el juicio de amparo en los

153. Baja California, Campeche, Coahuila, Chihuahua, Durango, Estado de México, Jalisco, Morelos, Michoacán, Puebla, Querétaro, San Luis Potosí, Tabasco y Tlaxcala.
154. Aguascalientes, Baja California Sur, Colima, Chiapas, Distrito Federal, Guanajuato, Guerrero, Hidalgo, Nayarit, Oaxaca y Quintana Roo.
155. Sonora.
156. LFPDPPP, artículo 39, sección VI.
157. Artículo 56 de la LFPDPP.
158. La LFPDPPP fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010, pero el ejercicio de los derechos de acceso, rectificación, cancelación y oposición contemplados en esta ley están en vigencia desde el 6 de enero de 2012, según el Reglamento de la mencionada ley.

tribunales federales. Las entidades federales, por otro lado, no tienen el recurso de apelación, pues en su caso, las resoluciones del IFAI son definitivas.[159/]

En el caso del sector público (durante el período del 12 de junio de 2003 al 31 de diciembre de 2011), el IFAI recibió un total de 4505 apelaciones de casos de datos personales. De éstos, 4373 derivaron de negativas de las entidades federales a permitir el acceso a datos personales en su posesión. Los otros 132 casos se referían a quejas relacionadas con la rectificación de información. Durante este período, el IFAI también recibió 11 quejas por el supuesto procesamiento inadecuado de datos personales por parte del sector público.

iv. Capacidades de investigación/procesamiento penal

La LFPDPPP dispone los procedimientos de cumplimiento: uno iniciado a solicitud del titular[160/] y el otro, un procedimiento de verificación, que puede ser iniciado petición del titular o por el IFAI cuando existen razones para sospechar la existencia de infracciones o a petición de parte.[161/]

El IFAI también tiene la facultad de llevar a cabo investigaciones y hacer recomendaciones sobre la protección de datos personales conforme a la LFTAIPG.[162/] Además, los esquemas de autorregulación vinculante requieren la certificación por parte del IFAI, el cual puede llevar a cabo "auditorías proactivas" en cualquier momento antes o después de otorgar dicha certificación. Para tales efectos, las certificadoras serán acreditadas para este propósito y llevarán a cabo la certificación de acuerdo con los parámetros establecidos para estos fines.[163/]

Conforme a las leyes mexicanas, las autoridades están facultadas para llevar a cabo investigaciones, y cualquier infracción a la ley puede ser objeto de acciones penales. Para el procesamiento de datos personales por parte de particulares, la ley federal establece el comportamiento ilícito que puede dar lugar a responsabilidades de carácter penal.[164/]

Las quejas relacionadas con el comercio ilegal de datos personales también pueden ser hechas ante el Ministerio Público, que es el órgano administrativo responsable de llevar a cabo investigaciones y ejercer acciones penales. Las entidades responsables de la observancia de las leyes en materia de privacidad, por un lado, y las entidades responsables de acciones penales, por el otro, están vinculadas por la necesidad de cooperar para determinar la existencia de una posible conducta criminal y si tal conducta puede ser objeto de acciones ante los tribunales.

---

159. LFTAIPG, artículo 37, sección II.
160. Artículos del 45 al 58.
161. Artículos del 59 al 60.
162. Artículos 37, secciones IX y XIX de la LFTAIPG; 2, sección V, y 6 del Reglamento, así como el numeral 43 de los Lineamientos de Protección de Datos Personales.
163. Artículos 83 y 84 del Reglamento de esta ley.
164. LFPDPPP, artículos 67 y 68.

C. Cooperación transfronteriza

i. Transferencia de datos

Las leyes mexicanas se restringen la transferencia de datos personales tanto en el territorio nacional como fuera de éste, y por lo general se requiere que la jurisdicción receptora esté sujeta a los mismos principios y derechos que gobiernan el procesamiento de datos personales conforme a la LFPDPPP, en particular la necesidad de observar los principios de aviso y consentimiento.[165/]

En el caso de transferencias nacionales, el Reglamento establece que el receptor de los datos personales será regulado por la ley y deberá tratar los datos personales conforme a lo convenido en el aviso de privacidad establecido por el receptor y el transferente.[166/]

En el caso de transferencias a otros países, la ley establece que éstas solo serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponderían al transferente.[167/]

ii. Instrumentos/acuerdos internacionales

Las leyes mexicanas confieren al IFAI la facultad de cooperar con otras autoridades nacionales e internacionales dedicadas a la protección de datos y la observancia de las leyes en la materia.[168/]

Aunque México no forma parte de ningún instrumento ni acuerdo relacionado con los principios internacionales de privacidad y flujos transfronterizos de información, el IFAI está comprometido a la protección de la privacidad y sus principios allende las fronteras; además, participa activamente en las labores relacionadas con la privacidad/protección de datos, flujos transfronterizos información y cooperación transfronteriza que se desarrollan actualmente en la OCDE, el APEC y el Consejo de Europa.

Sin embargo, cabe destacar que los instrumentos internacionales inciden en las prácticas y leyes mexicanas. Prueba de ello es el hecho de que tanto las Directrices de la OCDE que Rigen la Protección de la Privacidad y de los Flujos Transfronterizos de Datos Personales como el Marco de Privacidad del APEC fueron considerados en la redacción de la LFPDPPP. Asimismo, México participa activamente en el Grupo de Trabajo sobre Seguridad de la Información y Privacidad, pertenece al Subgrupo de Privacidad y al Grupo Ejecutivo de Comercio Electrónico, ambos del APEC, es observador del Consejo de Europa y fue aceptado por el Comité de Ministros del Comité Consultivo sobre la Modernización del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. México es miembro de la RIPD desde 2003 y desde 2010, la Comisionada Presidenta Jacqueline Peschard preside esta red.

México no ha recibido la certificación sobre privacidad/protección de datos de la Unión Europea. Sin embargo, uno de los objetivos del IFAI en el ámbito internacional es promover y apoyar

---

165. Artículos 36 y 37 de la LFPDPPP.
166. Artículos del 71 al 73 del Reglamento.
167. Artículo 74 del Reglamento de la LFPDPPP.
168. LFPDPPP (artículo 39, fracción VII).

a las autoridades nacionales para que inicien su proceso de certificación ante la Comisión Europea. En este sentido, la Secretaría de Relaciones Exteriores de México, encargada de solicitar el proceso de adecuación, está colaborando activamente en este esfuerzo.

iii. Cooperación en materia de investigación y ejecución de las leyes

En términos generales, el marco jurídico confiere a las autoridades de las diversas entidades de Gobierno la facultad de implementar los mecanismos para la difusión e intercambio de información con sus contrapartes en otros países. En materia penal, por ejemplo, la Secretaría de Seguridad Pública y la Procuraduría General de la República (PGR), de conformidad con la Ley Orgánica de la PGR, están facultadas para intercambiar diversa información con sus homólogas en el extranjero.[169/] De igual modo, en materia administrativa, las leyes locales facultan a la Procuraduría Federal del Consumidor[170/] y a la Secretaría de Hacienda y Crédito Público para intercambiar información con gobiernos extranjeros.[171/]

Por lo que se refiere a la cooperación formal en mecanismos internacionales, México no forma parte formalmente de la red GPEN ni del acuerdo CPEA del APEC. Sin embargo, tanto el Gobierno mismo como el IFAI participan delegaciones de ambos mecanismos. Además, el IFAI ha sido uno de los principales promotores de la labor de la RIPD desde su creación y actualmente ocupa la presidencia de dicha red.

D. Jurisprudencia y retos especiales

En el ámbito federal así como en lo que se refiere a las resoluciones del IFAI, la jurisprudencia en México da certidumbre a la interpretación y alcance que el Poder Judicial Federal da a ciertos preceptos jurídicos, incluida la protección de la privacidad.

Existen varios retos significativos a la implementación de las leyes sobre privacidad/protección de datos en los campos de las comunicaciones, la banca electrónica y la protección de los niños, por mencionar unos cuantos.

La regulación de las redes sociales también presenta retos especiales tanto por el número de usuarios, por un lado, como por la dificultad de aplicar leyes locales a compañías establecidas fuera del territorio mexicano. Estos retos incluyen los temas de jurisdicción, elección de ley, computación en la nube, ya que estos requieren de la existencia de un diseño legislativo suficiente que permita generar criterios para la aplicación de leyes nacionales ante el fenómeno de la desmaterialización que ha generado la Internet y los correspondientes desarrollos sobre dicha plataforma.

Adicionalmente, la regulación de la computación en la nube conlleva retos importantes en las siguientes áreas: administración de la seguridad por parte de los proveedores de servicios; gestión de derechos; arquitectura de seguridad; monitoreo y administración de incidentes de seguridad; pruebas

---

169. Reglamento interno de la Secretaría de Seguridad Pública, artículo 26, disponible en www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/770061/archivo;y Ley Orgánica de la PGR, artículo 5, disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LOPGR.pdf.

170. Artículo 24 de la Ley Federal de Protección al Consumidor.

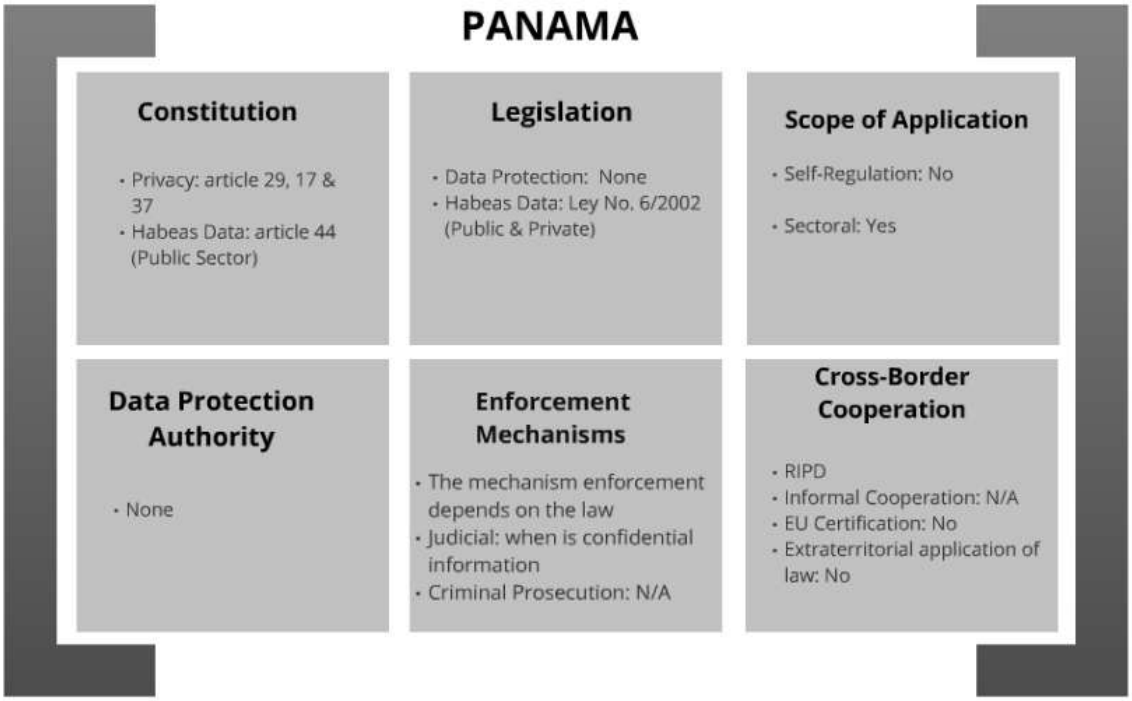
171. Artículos 15 A y 36 B de Reglamento de la SHCP.

y medidas de seguridad; capacitación del personal; transparencia; opciones de control para el usuario; portabilidad y uso de los datos personales; interoperabilidad; protección de datos y cumplimiento; certificación, y proveedores de servicios para la administración pública.

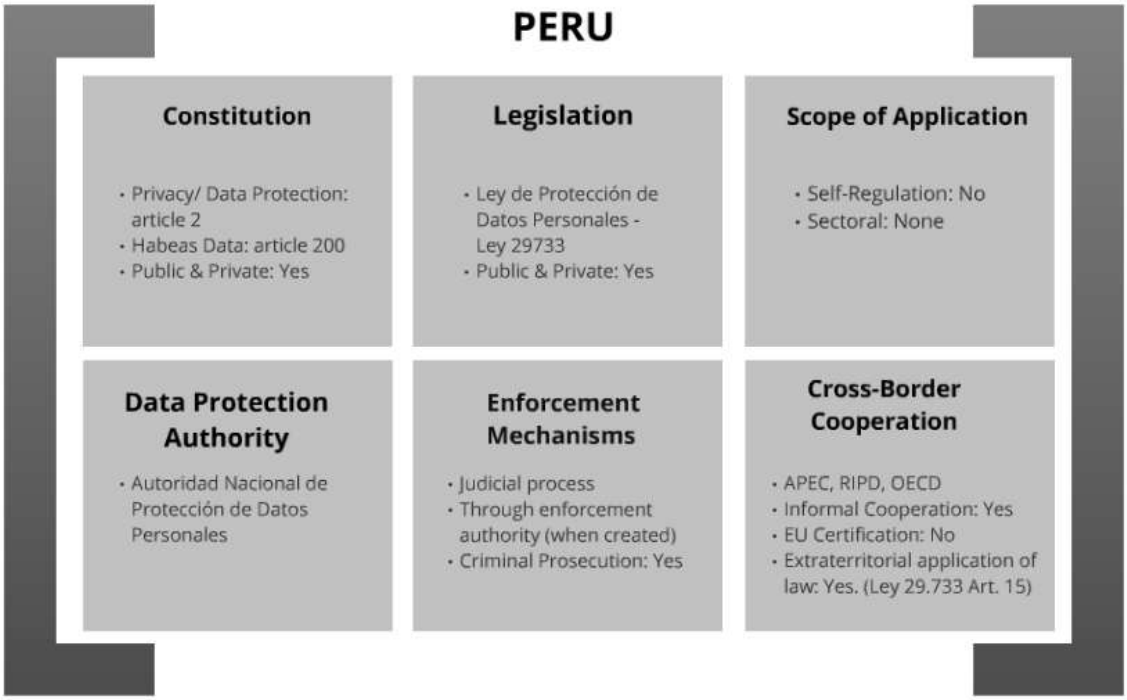
La regulación del mercadeo vía SMS, correo electrónico, MMS, llamadas telefónicas pregrabadas y faxes, entre otros, plantea también grandes desafíos para la regulación de las comunicaciones electrónicas. Lo mismo ocurre en los casos en que las empresas utilizan datos recabados de forma automática por Internet o a través de foros o grupos de noticias, listas de correo y datos en Internet.

Por último, un tema de particular interés es el de la vigilancia por video, que implica dos importantes intereses jurídicos trascendentes en México: la seguridad y la privacidad/protección de datos. En este caso, el reto es lograr un equilibrio entre el alcance y la importancia de cada uno de ellos.

8. Panamá



9. Perú



10. Estados Unidos

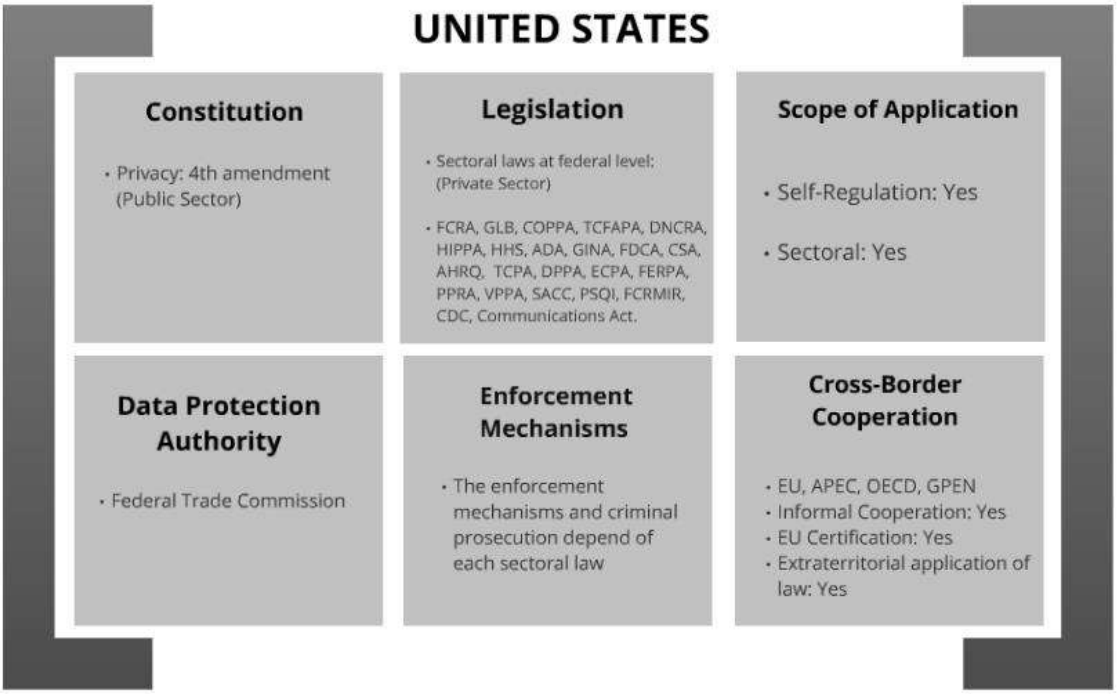
Las respuestas de Estados Unidos al Cuestionario de Legislación y Prácticas sobre Privacidad y Protección de Datos de la CAJP se encuentran en el documento CP/CAJP-3026/11 add. 9, y constituyen la base para la información que se resume en esta sección.

A. Contexto jurídico

i. Marco constitucional

La Cuarta Enmienda de la Constitución de Estados Unidos protege la libertad impidiendo cualquier injerencia arbitraria e ilícita en la privacidad del individuo. Dicha enmienda, con algunas excepciones, prohíbe al Gobierno realizar registros y decomisos irracionales. Se presumen irracionales los registros y decomisos si llevan a cabo sin una orden judicial, a no ser que se aplique una de las excepciones establecidas. Toda excepción deberá fundamentarse en que existe una causa probable para creer que se ha cometido, se cometerá o se está cometiendo un delito.

Por lo general, la Cuarta Enmienda no regula las infracciones a la privacidad por parte de entidades comerciales. Las constituciones de varios estados contienen referencias a la privacidad que pueden ser interpretadas de maneras diferentes por sus respectivos cuerpos judiciales.[172/]



ii. Marco legislativo

LEGISLACIÓN FEDERAL. En lo federal, se han promulgado diversas leyes sectoriales[173/], varias de las cuales entran dentro del ámbito de autoridad de la Comisión Federal de Comercio, la

172. *Véase* una lista de leyes estatales en National Conference of State Legislatures http://www.ncsl.org/issues-research/telecommunications-information-technology/privacy-protections-in-state-constitutions.aspx.

173. La información que se proporciona se refiere a las leyes sectoriales que corresponden más bien al sector privado o comercial y no al uso de datos personales por parte del Gobierno. Con respecto al uso de datos personales por parte del Gobierno, la International Association of Privacy Professionals ofrece un examen de certificación para profesionales en materia de privacidad especializados en el uso de datos personales por parte del Gobierno y ofrece una lista útil de las principales leyes en esta área. *Véase* https://www.privacyassociation.org/images/uploads/CIPP_G_BoK_01_2012.pdf . La Ley de Privacidad de 1974 es una de las principales leyes federales que protege la privacidad de la información en el sector público. Esta ley fue promulgada en respuesta a las inquietudes suscitadas con respecto a la creación y uso de bases de datos computarizadas y el impacto que éstas podrían tener en el derecho a la privacidad de los individuos. Protege la privacidad mediante la creación de cuatro derechos procedimentales y sustantivos en materia de datos personales. En primer lugar, establece que las entidades de Gobierno están obligadas a mostrar a cualquier persona los datos que sobre ella se conserven. En segundo lugar, establece que estas entidades deben guiarse por "principios justos en la recopilación y manejo de datos personales". En tercer lugar, restringe la forma en que estas entidades

cual tiene facultades en el área de privacidad comercial y vigila la aplicación de las siguientes leyes:[174]

Ley de la Comisión Federal de Comercio.[175] En la sección 5 de la Ley de la Comisión Federal de Comercio se confieren poderes amplios para que esta Comisión pueda combatir prácticas "injustas y engañosas". La Comisión Federal de Comercio aprovecha esta amplia potestad para proteger los intereses de los consumidores en materia de privacidad cuando ocurren serias infracciones por prácticas engañosas e injustas. Cuando ocurren violaciones a la sección 5 de esta ley, la Comisión Federal de Comercio puede conseguir la imposición de medidas cautelares, el pago de compensaciones por daños a consumidores, la restitución de ganancias mal habidas y algún otro tipo de desagravio equitativo.[176]

Ley de Imparcialidad en la Calificación de Crédito. [177] Esta ley tiene como objetivo proteger la información que recopilan las empresas calificadoras de crédito, las de información médica así como aquellas compañías que realizan investigaciones sobre candidatos a inquilinos o empleados. Conforme a esta ley, las empresas calificadoras de crédito no pueden proporcionar información a ninguna persona que no tenga un propósito específico y sancionado por la ley. Además, las personas que utilicen los informes para propósitos de crédito, seguro o empleo deben notificar al titular de los datos cuando se tome una acción adversa en función de dichos informes. Asimismo, los usuarios deben identificar a la empresa calificadora de crédito que haya proporcionado el informe de tal manera que el titular pueda impugnar o verificar la exactitud e integridad del informe. Esta ley regula asimismo a aquellas compañías que proporcionan información a las empresas calificadoras de crédito, imponiendo obligaciones jurídicas específicas sobre la precisión de la información, incluida la obligación de llevar a cabo una investigación sobre toda información que sea impugnada. Esta ley ha sido objeto de considerables enmiendas contenidas en la Ley de Transacciones de Crédito Imparciales y Precisas, la Ley de Tarjetas de Crédito y la Ley Dodd-Frank.

Ley Gramm-Leach-Bliley[178] La sección V, subsección A de la Ley Gramm-Leach-Bliley tiene como objetivo garantizar que las instituciones financieras protejan la privacidad de la información personal de los consumidores. En términos generales, esta ley, con las enmiendas de la Ley de Reforma Dodd-Frank Wall Street y Protección al Consumidor, autoriza a la Oficina de

---

pueden compartir los datos de una persona con terceros. En cuarto y último lugar, ofrece a los individuos la posibilidad de demandar al Gobierno cuando se infrinjan estas disposiciones. La Ley de Privacidad establece que la información sobre una persona debe ser pertinente y necesaria para un determinado propósito; además, debe ser precisa, oportuna y completa para garantizar su imparcialidad, y limita el uso de la información a los empleados y funcionarios de una entidad de Gobierno, siempre y cuando requieran esta información para el desempeño de sus funciones. Un análisis de la Ley de Privacidad de 1974, que regula principalmente al Poder Ejecutivo federal se encuentra en http://www.justice.gov/opcl/1974privacyact-overview.htm.

174. Sin embargo, la Comisión Federal de Comercio no tiene facultad para hacer cumplir algunas leyes contra ciertos tipos de entidades, por ejemplo los bancos. En estos casos, esta facultad recae en la entidad pertinente encargada de la legislación federal correspondiente a las actividades bancarias.
175. 15 U.S.C. § 41 et. seq.
176. 15 U.S.C. § 53(b).
177. 15 U.S.C. § 1681 et seq. enmendado, disponible en http://www.ftc.gov/os/statutes/031224fcra.pdf.
178. Pub. L.106-102, 113 Stat.1338, codificado en sus partes pertinentes en 15 U.S.C. §§ 6801-6809 y §§ 6821-6827, enmendada, disponible en http://www.law.cornell.edu/uscode/uscode15/usc_sec_15_00006801----000-.html.

Protección Financiera del Consumidor[179/] a establecer límites a la divulgación de información personal no pública por parte de instituciones financieras a terceros no afiliados. Conforme a esta ley y a las disposiciones de la Oficina de Protección Financiera del Consumidor, una institución financiera debe elaborar y dar a conocer sus avisos de privacidad a sus clientes por lo menos una vez al año. Además, las instituciones financieras no pueden divulgar ninguna información personal no pública sobre un consumidor a terceros no afiliados, a menos que la institución, en primer lugar, proporcione su aviso de privacidad al consumidor y, en segundo lugar, dé al consumidor la oportunidad de negar su consentimiento para que se divulgue su información, y que el consumidor no niegue su consentimiento. Esta ley impide expresamente que se divulgue un número de cuenta para propósitos de mercadeo. La subsección A de la sección V establece asimismo que la Comisión Federal de Comercio y otras entidades deben emitir disposiciones (*véase*, por ejemplo, 16 CFR Parte 314) para que las instituciones financieras protejan la información personal no pública. La subsección B de la sección V prohíbe la obtención de información de consumidores de una institución financiera con pretensiones falsas. En general, la Comisión Federal de Comercio se encarga de hacer valer las disposiciones de la sección V de la Ley Gramm-Leach-Bliley con respecto a las entidades no asignadas específicamente a la Oficina de Protección Financiera del Consumidor, las entidades bancarias federales u otras entidades reguladoras.

Ley de Protección de la Privacidad de los Niños en Línea.[180/] Esta ley protege la privacidad de los niños, dándoles a los padres las herramientas para controlar la información que se recopila sobre sus hijos en línea. Conforme al reglamento de esta ley[181/], los operadores de sitios web comerciales y los servicios en línea que de manera expresa recopilen información personal de niños menores de 13 años deben: (1) notificar a los padres sobre sus prácticas en materia de recopilación de datos; (2) obtener el consentimiento de los padres por medios verificables antes de recopilar la información personal de los niños; (3) dar a los padres la oportunidad de escoger si la información de sus hijos ha de ser compartida con terceros; (4) proporcionar a los padres acceso a la información sobre sus hijos; (5) permitir que los padres impidan cualquier uso ulterior de la información recopilada; (6) no solicitar a los niños más información de la que sea razonablemente necesaria para participar en una actividad, y (7) garantizar la confidencialidad, seguridad e integridad de la información.

Ley de Prevención del Abuso en Ventas por Teléfono y Fraude al Consumidor.[182/] Esta ley establece que la Comisión Federal de Comercio debe promulgar la normativa necesaria para (1) definir y prohibir los actos o prácticas engañosas en telemercadeo; (2) prohibir a las empresas dedicadas al telemercadeo que realicen llamadas que los consumidores consideren como indeseadas, coercitivas y una invasión a su privacidad; (3) restringir los horarios diurnos o nocturnos en que se pueden hacer este tipo de llamadas a los consumidores, y (4) establecer el propósito de la llamada

---

179. La Ley Gramm-Leach-Bliley faculta a la Comisión Federal de Comercio a emitir reglas para algunas instituciones financieras no bancarias; también faculta a la Comisión de Comercio de Mercados de Futuros y a la Comisión de Bolsa y Valores a emitir reglas para las instituciones financieras bajo la jurisdicción de esas entidades, respectivamente. Las tres comisiones mencionadas anteriormente se encargan de aplicar sus propias reglas sobre privacidad conforme a la Ley Gramm-Leach-Bliley.

180. 15 U.S.C. §§ 6501-6506; *véase* http://www.ftc.gov/privacy/coppafaqs.shtm.

181. Codificado en 16 C.F.R. Parte 312.

182. Codificado en la parte relevante de 15 U.S.C. §§ 6101-6108; disponible en http://www.law.cornell.edu/uscode/15/ch87.html. Las reglas de la Comisión Federal de Comercio pueden encontrarse en la Parte 310 del 16 C.F.R.

desde el principio de la misma si se trata de vender bienes y servicios. La ley autoriza expresamente a la Comisión Federal de Comercio a incluir en tal normativa a las entidades que "ayudan o facilitan" las prácticas engañosas de telemercadeo.

Ley del Registro Nacional No Llame:[183/] Esta ley faculta expresamente a la Comisión Federal de Comercio para que conforme a la sección 3(a)(3)(A) de la Ley de Prevención de Abuso en Ventas por Teléfono y Fraude al Consumidor implemente un mecanismo de registro mediante el cual se proteja la privacidad de los consumidores, permitiéndoles que eviten recibir llamadas de empresas de telemercadeo. La Comisión Federal de Comercio y la Comisión Federal de Comunicaciones monitorean juntas la observancia de esta disposición.

Ley de Control del Ataque por Pornografía y Mercadeo No Solicitado.[184/] Esta ley establece los requerimientos para aquellas personas que envían correos electrónicos no solicitados de naturaleza comercial, prohíbe el uso de información falsa o engañosa y también el uso de palabras engañosas en la línea del asunto de correos electrónicos. Establece también que en los mensajes de correo electrónico de carácter comercial no solicitados debe ofrecerse a los receptores la posibilidad de pedir que se les dejen de enviar tales mensajes, y que dicho mensaje sea identificado como anuncio comercial. La Comisión Federal de Comercio y la Comisión Federal de Comunicaciones están encargadas de vigilar la observancia de la Ley de Control del Ataque por Pornografía y Mercadeo No Solicitado.

Existen otras leyes relacionadas con la privacidad que rigen el sector privado que no entran dentro de la jurisdicción de la Comisión Federal de Comercio, entre las que pueden mencionarse las siguientes, de manera enunciativa más no limitativa:

Ley de Portabilidad y Responsabilidad de Seguros Médicos (conocido por sus siglas en inglés como HIPPA).[185/] La Ley HIPPA establece algunas protecciones de carácter federal para la información relacionada con la salud de los individuos en manos de "entidades cubiertas", entre los que se incluyen a los proveedores de servicios médicos, planes de salud y centros de coordinación de atención de la salud. Se aplica a las entidades cubiertas tanto del sector público como del privado. La cláusula de privacidad de esta ley establece las reglas sobre el uso y difusión que pueden hacer las entidades de la información relativa a la salud de individuos identificables, establece que la información debe estar protegida y da a los individuos ciertos derechos con respecto a la información de su salud, incluido el derecho a examinar y obtener una copia de sus expedientes médicos y a solicitar que se hagan correcciones. Por otra parte, la cláusula de seguridad de esta ley establece que las entidades deben implementar una serie de salvaguardas administrativas, físicas y técnicas para garantizar la confidencialidad, integridad y disponibilidad por medios electrónicos de la información

---

183. Ley del Registro Nacional No Llame de 2003 (15 U.S.C. § 6151; codificado originalmente en 15 U.S.C. § 6101 nota): http://www.gpo.gov/fdsys/pkg/USCODE-2010-title15/pdf/USCODE-2010-title15-chap87A-sec6151.pdf
184. Ley de Control del Ataque por Pornografía y Mercadeo No Solicitado, de 2003 (CAN-SPAM Act) (15 U.S.C §§ 7701-7713): http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf
185. Ley HIPPA y su reglamento promulgado por el Departamento de Salud y Servicios Humanos de Estados Unidos ("Cláusula de privacidad" y "Cláusula de seguridad"). Ley Pública 104-191; reglamentos del DSSH en 45 C.F.R., partes 160 y 164; copias disponibles en http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html.

protegida sobre la salud de los individuos. En 2009, la Ley de Tecnologías de la Información en la Salud para el Bienestar Económico y Clínico (Ley HITECH), que forma parte de la Ley de Recuperación y Reinversión, representó un fortalecimiento de las disposiciones sobre privacidad y seguridad ampliando, entre otras cosas, ciertos requerimientos directamente a los contratistas de las entidades cubiertas que manejan información personal sobre salud.

Regla sobre Notificación de Fallas de Seguridad en materia de Información de la Salud.[186/] Según esta regla, las entidades cubiertas tienen que avisar a los pacientes, al Departamento de Salud y Servicios Humanos y, en algunos casos, a los medios cuando se detecte una falla en los sistemas de protección de información sobre la salud. Los contratistas de las entidades cubiertas también tienen que notificar a las entidades para las que trabajen inmediatamente después de que se haya detectado la falla.

Regla sobre Notificación de Fallas de Seguridad en materia de Salud.[187/] Los proveedores de expedientes médicos personales y entidades vinculadas deben dar aviso a los consumidores cuando se detecte una falla en los sistemas de seguridad de información de la salud identificable mantenida en medios electrónicos. Si un proveedor de un proveedor de servicios de expedientes médicos personales experimenta una falla en sus sistemas de seguridad debe notificarlo de inmediato. El proveedor de expedientes médicos personales debe, a su vez, notificar a cada una de las personas afectadas, ciudadanos o residentes de Estados Unidos, a la Comisión Federal de Comercio y, en algunos casos, a los medios.

Ley de Estadounidenses con Discapacidades.[188/] En términos generales, esta ley prohíbe a los empleadores realizar exámenes médicos o investigar si un solicitante de empleo tiene alguna discapacidad o sobre la naturaleza o gravedad de una discapacidad, salvo en el caso de que la investigación que pretende hacerse esté específicamente relacionada con el trabajo que habrá de desempeñar el solicitante y que se justifique por necesidad del trabajo mismo. La Comisión para la Igualdad de Oportunidades en el Empleo (conocida por su sigla en inglés como EEOC) ha emitido reglas que disponen que la información recopilada sobre el estado o el historial de salud de un solicitante de empleo debe colocarse en formularios y expedientes separados y que deben ser considerados como confidenciales.[189/] La EEOC ha emitido reglas adicionales sobre las investigaciones relacionadas con el empleo.[190/]

---

186. Regla sobre Notificación de Fallas de Seguridad en materia de Información de la Salud (Departamento de Salud y Servicios Humanos) 45 CFR parte 160 y 45 CFR parte 164 subpartes A y D, disponible en http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.
187. Regla sobre Notificación de Fallas de Seguridad en materia de Salud (Comisión Federal de Comercio), 16 CFR parte 318, disponible en http://business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule.
188. Pub. L. 101-336, enmendada. Las secciones I y V de la Ley de Estadounidenses con Discapacidades están disponibles en línea en http://www.eeoc.gov/laws/statutes/ada.cfm.
189. 29 C.F.R. parte 1630, disponible en http://www.gpo.gov/fdsys/pkg/CFR-2011-title29-vol4/xml/CFR-2011-title29-vol4-part1630.xml. *Véase* en particular 29 C.F.R. § 1630.14(b)(1).
190. *Véase*, por ejemplo, Enforcement Guide: Preemployment Disability-Related Questions and Medical Examinations, EEOC NOTICE Number 915.002, 10/10/9, disponible en http://www.eeoc.gov/policy/docs/preemp.html.

Ley de No Discriminación por Información Genética.[191/] En términos generales, esta ley prohíbe que se discrimine a una persona tanto en la cobertura de seguro médico como en las oportunidades de empleo por su información genética. En la sección I de esta ley se prohíbe discriminar en los grupos de asegurados por razones de la información genética, prohíbe el uso de este tipo de información como base para determinar la eligibilidad o el monto de las primas en las pólizas de seguro individual o complementario del Medicare (Medigap), asimismo limita la disponibilidad de planes de seguro médico grupal, el número de aseguradoras, y el número de empresas participantes en el Medigap que pueden recopilar información genética o que pueden pedir o exigir que los asegurados se sometan a pruebas genéticas. Además de estas disposiciones antidiscriminatorias, la sección II prohíbe a los empleadores basar sus decisiones de contratación en la información genética de los candidatos y establece límites para tener acceso a este tipo de información. Impone asimismo ciertas obligaciones en materia de confidencialidad a los empleadores y otras entidades cubiertas (agencias de colocación, sindicatos y programas de capacitación) que posean información genética. El reglamento de esta ley fue emitido por la EEOC, el Departamento de Salud y Servicios Humanos, el Departamento del Tesoro y el Departamento del Trabajo.[192/]

Sección X de la Ley del Servicio de Salud Pública, Confidencialidad de la Información, Sección X.[193/] La Sección X de la Ley del Servicio de Salud Pública dispone el financiamiento para los servicios de planificación familiar. El estatuto y reglamento del programa relativo a la Sección X contiene las reglas referentes al consentimiento y confidencialidad encaminadas a reducir los obstáculos para la atención de la salud y proteger la privacidad de los adolescentes receptores de este tipo de servicios.

El reglamento de la Sección X establece que los proveedores de servicios que reciben fondos conforme a esta sección deben mantener en absoluta reserva "toda la información sobre hechos y circunstancias personales [de los pacientes] que obtenga el personal del proyecto". El reglamento prohíbe a los proveedores divulgar la información de los pacientes a menos que tenga la autorización por escrito del paciente, que sea necesario para otorgar servicios al paciente o porque así lo establezcan las leyes estatales o federales. Dispone asimismo que los proveedores de servicio deben establecer las "salvaguardas necesarias para proteger la confidencialidad". En caso contrario, la información podría ser divulgada en forma resumida, en forma de estadísticas o en alguna otra forma en la que no se identifiquen a los pacientes.

Oficina de Servicios de Abuso de Sustancias y Salud Mental. Confidencialidad de Expedientes de Pacientes de Abuso de Sustancias:[194/] Este reglamento prohíbe a los establecimientos financiados por el Gobierno federal dedicados al tratamiento de abuso de alcohol y sustancias que

---

191. *Véase* http://www.eeoc.gov/laws/types/genetic.cfm. Ley Pública 110-233, 122 Stat. 881, disponible en http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ233.110.pdf
192. *Véase* http://www.eeoc.gov/laws/types/genetic.cfm. Ley Pública 110-233, 122 Stat. 881, disponible en http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ233.110.pdf
193. 42 C.F.R. § 59.11, disponible en http://law.justia.com/cfr/title42/42-1.0.1.4.41.1.19.11.html.
194. 42 CFR Parte 2 y 42 USC § 290-dd-2, disponible en http://www.samhsa.gov/legislate/Sept01/01907_42cfr_part2.htm.

divulguen los expedientes de sus pacientes sin su consentimiento expreso y específico. La prohibición se hace extensiva a quienes reciben los datos pues no pueden divulgarlos a su vez sin antes obtener el permiso de los pacientes.

Requerimientos de Privacidad del Medicaid.[195/] Las normas federales de protección de datos del Medicaid fueron establecidas en el párrafo 1902(a)(7) de la Ley del Seguro Social [42 USC § 1396a(a)(7)]. Aquí se establece que un "plan estatal de asistencia médica debe: (7) establecer salvaguardas que restringen el uso y difusión de información sobre pacientes y receptores para propósitos directamente vinculados a la administración del plan". Este requerimiento se incrementa conforme al 42 CFR § 431.300 et seq.

Ley de Alimentos, Medicamentos y Cosméticos.[196/] Esta ley establece que ningún investigador podrá utilizar seres humanos como objeto de una investigación de las estipuladas en esta misma ley, a no ser que el investigador haya obtenido el consentimiento informado y legal del sujeto o de su representante legal debidamente autorizado. El investigador solicitará dicho consentimiento solo cuando el sujeto o su representante tengan el suficiente tiempo para considerar su participación y solo cuando se garantice que no existe la mínima posibilidad de coerción o intimidación. Al solicitar el consentimiento informado se dará a cada sujeto un escrito en el que se describa el grado, si corresponde, en que se habrá de proteger la confidencialidad de los expedientes en los que se identifique al sujeto y en el que se establezca la posibilidad de que la Oficina de Alimentos y Medicamentos inspeccione estos expedientes.

Ley de Sustancias Controladas.[197/] Con esta ley los encargados de una investigación pueden negarse a dar a conocer información con la que se identifique a los participantes en una investigación aunque ésta vaya a ser usada en juicios civiles, penales, administrativos, asuntos legislativos o de otra índole.

Política Federal para la Protección de los Sujetos Humanos (Regla Común).[198/] El Departamento de Salud y Servicios Humanos cuenta con reglamentos federales para la protección de sujetos humanos en investigaciones, que incluyen disposiciones relacionadas con la protección de la privacidad de sujetos de investigaciones y la confidencialidad de los datos relativos a éstos. En particular, la 45 CFR 46.111(a)(7) establece que para aprobar una investigación, una junta de revisión institucional debe determinar que "cuando corresponda, existan las disposiciones adecuadas para proteger la privacidad de los sujetos y la confidencialidad de los datos". Además, los reglamentos del Departamento de Salud y Servicios Humanos establecen que los sujetos deben estar informados de "las medidas que se habrán de tomar, si corresponde, para proteger los documentos en los que se los identifique" a no ser que la junta de revisión institucional haya concedido una dispensa para conseguir el consentimiento informado [45 CFR 46.116((a)(5)].

---

195. 42 CFR §§ 431.300-307 y 42 USC 1396a(a)(7), disponible en https://www.emedny.org/epaces/MedConfidentialityReg.aspx#Question_1.
196. 21 CFR Parte 50 disponible en http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=50.
197. 21 CFR § 1316.23 y 21 USC § 801, disponible en http://www.deadiversion.usdoj.gov/21cfr/cfr/1316/1316_23.htm y http://www.deadiversion.usdoj.gov/21cfr/21usc/801.htm.
198. 45 CFR § 46 subpartes de la A a la E; en particular 45 CFR § 46.111(a)(7) y 45 CFR § 46.116(a)(5), disponible en http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html.

Los reglamentos del Departamento de Salud y Servicios Humanos para la protección de sujetos humanos se aplican a cualquier institución que realice investigaciones no exentas con sujetos humanos y que sean llevadas a cabo con fondos proporcionados por el propio departamento. Además, los reglamentos del Departamento de Salud y Servicios Humanos también se aplican a investigaciones no exentas con sujetos humanos que no sean financiadas con recursos del propio departamento si tales investigaciones son llevadas a cabo por una institución estadounidense que voluntariamente haya optado por acatar tales reglamentos (por vía de un documento de garantía aprobado por la Oficina para la Protección de Seres Humanos en Investigaciones) en todas las investigaciones que lleve a cabo. Sin embargo, no se requiere una extensión de los reglamentos del Departamento de Salud y Servicios Humanos. Además del Departamento de Salud y Servicios Humanos, otros 14 departamentos y entidades federales han adoptado diversas reglas estandarizadas para la protección de sujetos humanos.[199/]

Autorización Reglamentaria para Certificados de Confidencialidad.[200/] Conforme a la sección 301(d) de la Ley del Servicio de Salud Pública [42 U.S.C. 241(d)], el Secretario de Salud y Servicios Humanos puede autorizar a personas vinculadas con investigaciones biomédicas, conductuales, clínicas o de otro tipo para que protejan la privacidad de los sujetos de dichas investigaciones impidiendo que personas ajenas a tales investigaciones tengan acceso a los nombres u otros datos que identifiquen a los sujetos. Las personas autorizadas por los Institutos Nacionales de Salud (conocidos por sus siglas en inglés como NIH) para proteger la privacidad de los sujetos de investigaciones no pueden ser obligadas en ningún proceso civil, penal, administrativo, legislativo o de otra índole, en los ámbitos federal, estatal o local, a identificarlos por nombre o por alguna característica.

Los certificados pueden ser utilizados para investigaciones biomédicas, conductuales, clínicas o de otro tipo que sean delicadas en naturaleza, lo que significa que si se divulga la identidad de los sujetos podría haber consecuencias adversas para estos o daños a su condición financiera, sus posibilidades para conseguir empleo o seguro, o para su reputación.

Ley de Seguridad del Paciente.[201/] Esta ley establece un sistema voluntario mediante el cual hospitales, médicos y otras instituciones que prestan servicios de salud pueden proporcionar información sobre la seguridad de los pacientes, la cual será recopilada, analizada y utilizada para resolver cualquier asunto relacionado con la seguridad de los pacientes y la calidad de los servicios que reciben. Con el objetivo de fomentar la presentación de informes y análisis de errores médicos, la Ley de Seguridad del Paciente establece algunas protecciones y privilegios de carácter federal para mantener en secreto la información del paciente que se genere y recopile en cualquier evento relacionado con la seguridad del paciente.

Las disposiciones de confidencialidad mejorarán la seguridad del paciente, creando un entorno en el que los proveedores pueden generar informes y analizar eventos sin crear temor de un aumento en los riesgos de responsabilidad ante terceros. Con estas disposiciones se pretende que al

---

199. http://www.hhs.gov/ohrp/humansubjects/commonrule/index.html.
200. 42 U.S.C. 241(d), disponible en http://www.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000241----000-.html.
201. Ley de Seguridad del Paciente y Mejora de la Calidad de 2005 (Ley de Seguridad del Paciente); 42 U.S.C. § 299b-21 a 299b-26 y Ley Pública 109-41 109 Congreso, disponible en http://codes.lp.findlaw.com/uscode/42/6A/VII/C/299b-21 y http://www.pso.ahrq.gov/statute/pl109-41.htm (ley pública).

aumentar el número de análisis e informes sobre cualquier evento relacionado con las del paciente se mejore la percepción de tales eventos.

Reglamentación sobre datos médicos para garantizar la imparcialidad en la calificación de crédito.[202/] Bajo ninguna circunstancia ningún acreedor puede obtener ni utilizar información médica para determinar si un consumidor es sujeto de crédito o no, salvo lo que estipule la Ley de Transacciones de Crédito Imparciales y Precisas. En términos generales, un acreedor no puede obtener ni usar información médica para determinar si un consumidor puede continuar gozando de un crédito o adquirir otro, siempre y cuando: (i) la información sea similar a la que se utiliza para determinar el otorgamiento de un crédito, por ejemplo datos relacionados con deudas, gastos, ingresos, beneficios, activos, garantías, o el propósito del préstamo, incluso el uso de las ganancias; (ii) el acreedor utilice la información médica de tal manera y en la medida que no resulte ser menos favorable que si utilizara información no médica en una transacción de crédito, y (iii) el acreedor no tome en cuenta la salud física ni mental, ni el historial médico ni el tipo de tratamiento ni el pronóstico del paciente para tomar una decisión sobre un crédito.

Disposiciones en materia de confidencialidad de la Agencia para la Investigación y la Calidad de la Atención de Salud.[203/] La Agencia para la Investigación y la Calidad de la Atención de Salud no puede utilizar los datos que recopila para ningún propósito diferente de aquel por el cual ha recopilado los datos a menos que la institución, persona o el proveedor de los datos haya dado su consentimiento expreso. Las personas que violen esta disposición están sujetas a una pena administrativa de hasta US$10.000.

Disposiciones en materia de confidencialidad de los Centros para el Control y la Prevención de Enfermedades (CDC).[204/] Los datos o información identificable deben ser utilizados exclusivamente para el propósito para el que fueron recopilados, a no ser que la entidad o persona identificada en los datos haya dado su consentimiento expreso, según lo determinen las reglas emitidas por el Secretario.

Ley de Comunicaciones de 1934 (enmendado):[205/] La Ley de Comunicaciones, puesto en ejecución por la Comisión Federal de Comunicaciones, proteger la confidencialidad y seguridad de los datos de consumidores recopilados por los proveedores de servicio a través de sus redes, incluidos los portadores de telecomunicaciones, proveedores de VoIP, de cable y satélite. Esta ley impone a los proveedores de servicios de comunicaciones el deber de mantener confidencial la información personal de los consumidores y limita sus facultades para utilizar y divulgar dicha información.[206/] Además, la Comisión Federal de Comunicaciones prohíbe a los portadores de servicios de telefonía dar a conocer el número del originador de una llamada a la parte receptora cuando el originador ha pedido expresamente que se le mantenga en anonimato.[207/] Esta ley prohíbe también la intercepción no autorizada y publicación de comunicaciones que se hagan por cable o radio.

---

202. 12 CFR Parte 717, disponible en http://www.access.gpo.gov/nara/cfr/waisidx_06/12cfr717_06.html.
203. 42 U.S.C. § 299c-3(d) disponible en http://codes.lp.findlaw.com/uscode/42/6A/VII/D/299c-3. *Véase* también http://www.ahrq.gov/fund/datamemo.htm.
204. 42 U.S.C. § 242m(d) disponible en http://www.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000242---m000-.html.
205. 47 U.S.C. § 151 et seq., disponible en http://transition.fcc.gov/telecom.html.
206. 47 U.S.C. §§ 222, 338(i), 551.
207. *Véase* 47 C.F.R. § 64.1601(b).

Ley de Protección del Consumidor por Teléfono[208/], enmendada por la Ley para la Prevención de Fax Basura[209/] y la Ley de Control del Ataque por Pornografía y Mercadeo No Solicitado.[210/] Estos estatutos protegen a los consumidores de llamadas telefónicas y fax no solicitados, así como de mensajes comerciales en correo electrónico no solicitados. Según la Ley de Protección del Consumidor por Teléfono, la Comisión Federal de Comunicaciones establece límites para las llamadas para promover productos o servicios o solicitar donativos a números residenciales, por ejemplo prohíbe el realizar este tipo de llamadas antes de las 8:00 a. m. o después de las 9:00 p. m., y exige que los vendedores por teléfono acaten las solicitudes expresas de los propietarios de no hacer llamadas. Tanto esta ley como la Comisión prohíben también la realización de llamadas grabadas o la realización de llamadas mediante marcación automática, así como el envío de mensajes de texto, independientemente de su contenido, a cualquier teléfono inalámbrico sin el consentimiento expreso del receptor, y prohíbe la realización de llamadas de telemercadeo grabadas a un número residencial sin el consentimiento del receptor. El Ley para la Prevención de Fax Basura prohíbe el envío de anuncios por fax no solicitados sin la invitación o permiso expreso del receptor, a no ser que el remitente haya establecido previamente una relación comercial con el receptor, y establece además que todos los anuncios por fax deben ofrecer claramente a su receptor la opción para suspender envíos futuros. El Ley de Control del Ataque por Pornografía y Mercadeo No Solicitado prohíbe el envío de mensajes de correo electrónico no solicitado a dispositivos inalámbricos sin el permiso previo correspondiente. La Comisión Federal de Comunicaciones es la encargada de poner en práctica estas disposiciones en colaboración con la Comisión Federal de Comercio.[211/]

Ley de Protección y Privacidad de Conductores de 1994.[212/] Esta ley protege la información personal de los individuos por los departamentos de vehículos automotores de los respectivos estados. Limita la divulgación de esta información personal a ciertos "usos permisibles" y requiere el consentimiento de la persona para la venta o divulgación de tal información por parte de usuarios autorizados, incluidas empresas, para propósitos diferentes de los "usos permisibles".

Ley de Privacidad de las Comunicaciones Electrónicas.[213/] Esta ley contempla, entre otras cosas, el acceso a los expedientes de comunicaciones electrónicas o por cable, y el uso de dispositivos de identificación de las comunicaciones de entrada y salida. En términos generales, prohíbe el acceso no autorizado o la difusión de comunicaciones electrónicas y por cable almacenadas en casos específicos; dispone también los procedimientos jurídicos que las autoridades pueden utilizar para conseguir tales comunicaciones y expedientes. Estas disposiciones prohíben el uso o instalación de dispositivos de identificación de las comunicaciones de entrada y salida, salvo en algunos casos especificados en esta ley. Salvo en circunstancias muy limitadas, las autoridades no

---

208. Codificado como 47 U.S.C. § 227.
209. *Íd.*
210. 15 U.S.C. 7701, et seq., Ley Pública N.° 108-187.
211. La Comisión Federal de Comercio se encarga también de administrar el Registro Nacional No Llame con el cual se permite a los consumidores limitar las llamadas de telemercadeo que reciben. La Comisión Federal de Comercio, la Comisión Federal de Comunicaciones y otras entidades estatales se encargan de velar por el cumplimiento del Registro Nacional No Llame.
212. 18 U.S.C. § 2721 et seq.
213. Codificado en 20 U.S.C. § 1232g *et seq.*); 34 C.F.R. parte 99 (implementación de la FERPA). *Véase* también la Ley de Educación para Personas Discapacitadas de 1970, enmendada a través de la Ley de Mejora en la Educación para los Individuos con Incapacidades de 2004, Sección I de la Ley Pública 108-446 (codificada en 20 U.S.C. § 1400 *et seq.*), en particular 20 U.S.C. § 1412(a)(8).

pueden instalar dispositivos de identificación de las comunicaciones de entrada y salida sin una orden previa de algún tribunal.

Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad.[214/] Esta ley se aplica a las entidades e instituciones educativas que reciben fondos de cualquier programa gestionado por el Departamento de Educación. Protege la privacidad de los estudiantes al establecer que las escuelas no podrán negar a los padres, por práctica o política, el derecho a conocer y analizar los expedientes de sus hijos en un plazo de 45 días después de haber presentado una solicitud o de solicitar su corrección cuando consideren que son inexactos. De acuerdo con esta ley, los padres también tienen derecho a dar su consentimiento para que se divulguen los datos de los expedientes con los que se puede identificar a los alumnos, salvo en los casos estipulados por la ley. Estos derechos se transfieren al estudiante al cumplir 18 años de edad o cuando ingrese a una institución de educación postsecundaria a cualquier edad ("estudiante elegible").

Enmienda a la Protección de los Derechos del Alumno.[215/] Esta enmienda otorga a los padres algunos derechos con respecto a las encuestas, análisis o evaluaciones en las que participen los estudiantes, relativos a una o más de las ocho áreas protegidas, incluso la conducta ilegal, antisocial, autodiscriminatoria o degradante, conducta o actitudes sexuales, o afinidades o creencias políticas del estudiante o de su familia. En el caso de encuestas financiadas por el Departamento de Educación, los padres tienen derecho a inspeccionar y revisar la encuesta y otorgar su consentimiento antes de que los estudiantes puedan contestar a ella. Si se trata de encuestas no financiadas por el Departamento de Educación pero que son llevadas a cabo por las escuelas al amparo de otros programas del propio departamento, las escuelas deben dar a los padres la oportunidad de inspeccionar y revisar la encuesta y también debe permitírseles solicitar que sus hijos sean excluidos de participar en ella. Esta enmienda también abarca encuestas de mercadotecnia y de otro tipo que incidan en la privacidad de los estudiantes, el acceso de los padres a la información y la administración de ciertos exámenes físicos a menores de edad. Los derechos conferidos a través de esta enmienda se transfieren de los padres al estudiante cuando éste cumple 18 años u obtiene su emancipación conforme a las leyes estatales.

Ley de Protección de la Privacidad en Video.[216/] Esta ley se aplica a las empresas dedicadas al arrendamiento, venta o entrega de videos pregrabados, a quienes les impiden divulgar registros sobre el arrendamiento o compra de videos con los que se pueda fácilmente identificar a una persona sin el previo consentimiento por escrito de ésta. Establece que estas empresas deben destruir la información que esté en su poder en el plazo de un año a partir del momento en que dejen de utilizarla.

El 23 de febrero de 2012, el Gobierno del Presidente Obama publicó un informe oficial sobre la privacidad de datos comerciales en el que se plantea la conveniencia de una Carta de Derechos del Consumidor en materia de Privacidad.[217/] Se pide al Congreso que emita esta carta y que además otorgue a la Comisión Federal de Comercio y a los fiscales estatales la facultad de ponerla en práctica

---

214. 20 U.S.C. § 1232g.
215. 20 U.S.C. § 1232h; 34 CFR parte 98.
216. 18 U.S.C. § 2710.
217. "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", febrero de 2012, disponible en http://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("White Paper").

directamente. En dicho informe se pide también el establecimiento de una norma nacional para la notificación de casos de fallas en la seguridad de datos, sin necesidad de contar con una legislación estatal en la materia.[218/]

LEGISLACIÓN ESTATAL: Varios estados han adoptado leyes relacionadas con la privacidad de datos y 47 estados, el Distrito de Columbia y varios territorios tienen leyes relativas a la notificación de fallas en los sistemas de seguridad de datos.[219/] En términos generales, en los 50 estados que integran Estados Unidos se tienen diversas leyes sobre privacidad/protección de datos referentes al acceso de los pacientes a sus expedientes médicos, restricciones a la divulgación de datos identificables en expedientes médicos, reglas sobre los privilegios de confidencialidad de expedientes de comunicaciones entre pacientes y profesionales del cuidado de la salud, incluidos los profesionales en salud mental, y algunas leyes específicas referentes a ciertas enfermedades. Si se desea ver un informe detallado sobre las leyes estatales en materia de privacidad en el área de la salud, *véase* el análisis en dos volúmenes de estatutos sobre privacidad estatales titulado "The State of Health Privacy".[220/]

El reciente informe oficial del Gobierno del Presidente Obama reconoce específicamente la importancia de los fiscales estatales como recurso en el área del cumplimiento de las leyes en materia de privacidad y solicita al Congreso de Estados Unidos que promulgue una ley con la que se faculte a la Comisión Federal de Comercio y a los fiscales estatales para publicar cartas de derechos de los consumidores en materia de privacidad.[221/]

---

218. White Paper, en págs. 35-39.

219. El Consejo Nacional de Legislaturas Estatales tienen un sitio web en el que se proporciona información sobre las leyes en materia de privacidad y notificación de fallas en los sistemas de protección de datos: http://www.ncsl.org/default.aspx?TabID=756&tabs=951,71,539#951. Muestra de leyes estatales representativas: Minnesota statutes on internet privacy §§ 325M.01 to .09: http://www.revisor.leg.state.mn.us/stats/325M; Nevada statute on privacy requirements for internet service providers § 205.498, disponible en: http://www.leg.state.nv.us/NRS/NRS-205.html#NRS205Sec498; California requirements on disclosures for third party sharing §§ 1798.83 to .84: disponible en http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84; California's Online Privacy Protection Act §§ 22575-22578, disponible en: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579; Utah requirements on disclosures for third party sharing §§ 13-37-101, -102, -201, -202, -203; disponible en: http://le.utah.gov/~code/TITLE13/13_37.htm; Delaware requirements for employer notice of email/Internet monitoring § 19-7-705, disponible en: http://delcode.delaware.gov/title19/c007/sc01/index.shtml#705; Connecticut requirements for employer notice of electronic monitoring § 31-48d, disponible en: http://www.cga.ct.gov/2011/pub/chap557.htm#Sec31-48d.htm; Connecticut privacy policy requirement § 42-471, disponible en: http://www.cga.ct.gov/2011/pub/chap743dd.htm#Sec42-471.htm; Nebraska requirement related to statements in privacy policies § 87-302(14), disponible en: http://uniweb.legislature.ne.gov/laws/statutes.php?statute=87-302; Pennsylvania requirement related to statements in privacy policies 18 Pa. C.S.A. § 4107(a)(10), disponible en: http://government.westlaw.com/linkedslice/default.asp?SP=pac-1000.

220. Disponible en http://hpi.georgetown.edu/privacy/publications.html.

221. White Paper, en págs. 37-38.

iii. Habeas data

Las leyes de Estados Unidos no prevén la figura del recurso del habeas data. No obstante, el derecho a conocer la información personal es un componente ampliamente conocido de los Principios de Imparcialidad en materia de Privacidad de la Información, establecidos originalmente por el Departamento de Salud, Educación y Bienestar a principios de los años 70, por lo que casi todas las leyes federales y estatales en materia de privacidad detalladas anteriormente hacen referencia al derecho de acceso.[222/]

La cláusula de privacidad de la Ley HIPAA otorga a los individuos el derecho a conocer sus expedientes médicos y otros expedientes relacionados con su salud en manos de entidades públicas y privadas vinculadas con la Ley HIPAA, incluidos los proveedores de servicios de atención médica, planes de salud y centros de coordinación de la atención de la salud.

La presentación de pruebas que conlleva todo proceso civil en Estados Unidos es también un método importante para conocer la información sobre uno mismo. La regla 26 del Código Federal de Procedimiento Civil dispone que las "partes pueden conseguir pruebas en cualquier asunto no confidencial que sea pertinente para los alegatos o defensa de cualquiera de las partes, incluida la existencia, descripción, naturaleza, custodia, condición y ubicación de cualquier documento o cualquier otro objeto tangible y la identidad y ubicación de las personas que tengan conocimiento de cualquier cosa que pueda ser utilizada como prueba".[223/]

Por último, la Ley sobre Libertad de Información y varias leyes estatales (conocidas en ocasiones como "leyes de transparencia pública" o "leyes de gobierno abierto") permiten también a los individuos conocer los datos sobre sí mismos y contribuyen a fomentar la transparencia en la toma de decisiones gubernamentales.[224/]

iv. Autoregulación

Por lo general, la Comisión Federal de Comercio ha considerado la autorregulación como un instrumento viable en diferentes áreas. La autorregulación es vista favorablemente por varias razones, entre las que se incluyen (i) la relativa velocidad y flexibilidad con la que se pueden elaborar y adaptar las reglas a las circunstancias cambiantes (en oposición a las leyes) y (ii) el hecho de que los representantes de las industrias tienen los conocimientos especializados necesarios para elaborar las normas pertinentes para una determinada industria. Cabe hacer notar que el término "autorregulación" no implica la falta de los conceptos de aplicabilidad y vigilancia. Cuando una empresa manifiesta públicamente que adopta cualquier código de conducta autorregulatorio, se obliga a cumplirlo conforme a la Ley de la Comisión Federal de Comercio que prohíbe toda práctica injusta y engañosa. El incumplimiento se considera como un engaño para los consumidores. Así pues, la "autorregulación" en este contexto también puede describirse como "corregulación".

---

222. 15 U.S.C. § 1681g, disponible en http://www.ftc.gov/os/statutes/031224fcra.pdf., y *véase* por ejemplo, la sección 609 de la Ley de Imparcialidad en la Calificación de Crédito (Avisos a los consumidores).
223. FRCP Rule 26 Duty to Disclose, disponible en http://www.law.cornell.edu/rules/frcp/rule_26.
224. *Véase* un resumen de las leyes estatales en http://sunshinereview.org/index.php/State_sunshine_laws.

Entre las iniciativas de la industria se incluyen, por ejemplo, el Código de Conducta de la Asociación de Mercadotecnia Móvil[225/] y el de la Oficina de Publicidad Interactiva.[226/] La Alianza de Publicidad Digital, una coalición de asociaciones de medios y mercadotecnia, ha adoptado una serie de principios autorregulatorios para la publicidad en línea y mejores mecanismos para la publicidad dirigida según el comportamiento de los consumidores. Tres de los principales proveedores de navegadores –Mozilla, Microsoft y Apple– anunciaron recientemente la elaboración de nuevos mecanismos objetivos para este tipo de publicidad con los que se pretende aumentar la transparencia, dar mayor control a los consumidores y mejorar la facilidad de uso. Recientemente, Mozilla introdujo también una versión de su navegador que permite no rastrear el comportamiento del usuario en un navegador utilizado en un aparato móvil. La Alianza de Publicidad Digital ha establecido también un programa de monitoreo gestionado a través del Better Business Bureau. El 22 de febrero de 2010, la Alianza de Publicidad Digital anunció que empezaría a trabajar de inmediato para agregar una serie de herramientas en los navegadores para que los consumidores pudieran expresar sus preferencias conforme a los principios de la propia alianza.[227/] Algunos actores también se han unido para formar un grupo de trabajo conocido como World Wide Web Consortium para elaborar las normas de los mecanismos para impedir el rastreo.

El organismo del sector privado de marcas de confianza, TRUSTe, cuenta con un programa con el que se certifican las políticas de privacidad de los sitios web, los monitorea y ofrece mecanismos para la solución de problemas. Si alguna empresa llega a infringir los requerimientos del programa TRUSTe podría perder el sello de confianza que otorga este organismo e incluso podría ser remitida a las autoridades de Gobierno pertinentes. Del mismo modo, el sello en línea que otorga el Better Business Bureau incluye requerimientos para la seguridad y privacidad de los datos.

La Ley de Protección de la Privacidad en Línea de los Niños y su reglamento (*véase* arriba) disponen esquemas autorregulatorios y mecanismos de seguridad aprobados por la Comisión Federal de Comercio. En la actualidad existen cuatro programas de seguridad cuyo objetivo principal es asegurar que sus miembros cumplan con lo establecido en la ley, aunque la ejecución de este corresponde plenamente a la Comisión Federal de Comercio. El mecanismo de seguridad está siendo revisado en este momento.

Además de estos códigos de conducta, el Gobierno de Estados Unidos ha participado en la elaboración de códigos de conducta encaminados a mejorar la interoperabilidad entre diversos regímenes de privacidad en el ámbito internacional. El Marco de Seguridad Estados Unidos-Unión Europea[228/] puede citarse como un ejemplo de un esfuerzo para implementar códigos de conducta y privacidad entre países. Este marco fue elaborado por el Departamento de Comercio de Estados Unidos en consulta con la Comisión Europea con la finalidad de ofrecer a las empresas estadounidenses un medio simplificado para cumplir con la Directiva sobre Protección de Datos de la

---

225. *Véase* http://mmaglobal.com/policies/code-of-conduct.
226. *Véase* http://www.iab.net/public_policy/codeofconduct.
227. Comunicado de prensa de la Alianza de Publicidad Digital, 22 de febrero de 2012, disponible en http://www.aboutads.info/resource/download/DAA_Commitment.pdf. *Véase* también "White House Unveils 'One-Click' Privacy Plan," Bangkok Post, 23 de febrero de 2012, disponible en http://www.bangkokpost.com/tech/computer/281239/white-house-unveils-one-click-privacy-plan; "No me sigas," El País, 23 de febrero de 2012, disponible en http://tecnologia.elpais.com/tecnologia/2012/02/23/actualidad/1329984921_916013.html.
228. Documentos en línea en http://export.gov/safeharbor/.

Comisión Europea. Este mecanismo fue aprobado en el año 2000 y un acuerdo similar, el Marco de Seguridad Estados Unidos-Suiza, fue finalizado en 2009. Ambos mecanismos han ayudado a salvar las diferencias entre Estados Unidos y los países de la Unión Europea en materia de protección de datos y han permitido a miles de compañías transferir datos entre ambas partes para así apoyar el comercio trasatlántico. Como ocurre con los la mayoría de los códigos de conducta, la participación por parte de las empresas estadounidenses en estos mecanismos de seguridad es totalmente voluntaria. Aquellas empresas que desean participar en ellos deben cumplir con los requisitos establecidos y certificar de *motu proprio* su cumplimiento cada año ante el Departamento de Comercio. Este marco incluye principios sobre avisos, elecciones, transferencia, acceso, seguridad, integridad de datos y aplicabilidad de las leyes. Como parte de sus obligaciones en este programa de seguridad, los organismos deben contar con procedimientos para verificar el cumplimiento de compromisos y un sistema independiente para investigar y resolver controversias. Tanto en la Comisión Federal de Comercio como el Departamento de Transporte están facultadas para verificar que los organismos cumplan los compromisos adquiridos en este marco, en particular las empresas de transporte aéreo y los agentes de boletos.

El 13 de noviembre de 2011, el Presidente Obama y los representantes de los países integrantes del APEC avalaron el Sistema de Reglas Transfronterizas sobre Privacidad, en una reunión en Honolulu, Hawai. Se trata de un código de conducta autorregulatorio encaminado a crear un sistema de protección más uniforme para los consumidores cuando sus datos son transferidos de un país a otro en la región del APEC, con diferentes regímenes. Las compañías que deseen participar en este sistema del APEC tendrán que pasar por un proceso de revisión y certificación a cargo de terceros, que examinarán sus políticas y prácticas de privacidad y velarán por la implementación de las nuevas reglas. Las autoridades en materia de seguridad en la región del APEC que decidan participar en el programa serán los principales encargados de hacer valer las reglas.

En el informe oficial del Gobierno del Presidente Obama también se pidió al Congreso que aprobara una ley para complementar el marco jurídico existente en materia de privacidad. Además, con la finalidad de hacer frente a los retos que plantea la rápida evolución de la tecnología, el Gobierno del Presidente Obama quiere aprovechar la experiencia y conocimientos del sector privado y conocer sus prácticas óptimas con el objeto de crear códigos de conducta voluntarios que promuevan el consentimiento informado y la protección de la información personal. Se prevé la participación de diversos actores interesados en la elaboración de estos códigos, con la salvedad de que los actores comerciales y no comerciales participarían de manera voluntaria. En última instancia, estos actores tienen la opción de adoptar o rechazar un determinado código de conducta. Sin embargo, las empresas estadounidenses saben que una vez que adopten un código de conducta estarán obligados a manejar los datos personales conforme lo indica la ley y bajo la supervisión de la Comisión Federal de Comercio.

B. Ejecución

i. Mecanismos de ejecución y recursos

Las leyes en materia de privacidad/protección de datos en los ámbitos federal y estatal disponen los siguientes derechos específicos de acción, procedimientos y recursos:

Ley de la Comisión Federal de Comercio. Cuando ocurren violaciones a la sección 5 de esta ley, que prohíbe toda práctica injusta y engañosa, la Comisión Federal de Comercio puede conseguir la imposición de medidas cautelares, el pago de compensaciones por daños a consumidores, la restitución de ganancias mal habidas y algún otro tipo de desagravio equitativo.

Ley de Imparcialidad en la Calificación de Crédito. Esta ley dispone penas de carácter civil por faltas dolosas o culposas, y los recursos que establece son también más estrictos.[229/] Dispone asimismo sanciones penales para los casos en que se recurra a engaños para conseguir datos sobre consumidores.[230/]La aplicación de esta ley está cargo de las autoridades federales y estatales, y también de actores privados. Permite a los tribunales imponer multas de hasta US$3500 en casos de transgresiones dolosas presentadas ante la Comisión Federal de Comercio.[231/]

Ley Gramm-Leach-Bliley. Esta ley dispone que la aplicación administrativa corresponde a las autoridades federales y estatales. En general, la Oficina de Protección Financiera del Consumidor está facultada para hacer valer las disposiciones en materia de privacidad (pero no las disposiciones en materia de seguridad de datos) de esta ley con respecto a una entidad contemplada en la misma, excepto por las entidades reguladas por la Comisión de Comercio de Mercados de Futuros, la Comisión de Bolsa y Valores, o un regulador estatal de seguros. Además, la Comisión Federal de Comercio está facultada para hacer cumplir la Ley Gramm-Leach-Bliley con respecto a una entidad contemplada en esta ley, con excepción de aquellas reguladas por una entidad federal o por un regulador estatal de seguros. La Ley Gramm-Leach-Bliley permite a cada entidad federal o estatal autorizada procurar los recursos o imponer penas por infracciones, cuyo tipo y magnitud dependerá de las facultades específicas que les hayan sido otorgadas.[232/]

Ley de Protección de la Privacidad en Línea de los Niños: Según esta ley, toda práctica injusta o engañosa es considerada como una infracción. La Comisión Federal de Comercio, otros reguladores federales y autoridades estatales están encargados de hacer valer las disposiciones de esta ley. Toda infracción conlleva sanciones económicas.

Ley de Telemercadeo.[233/] La Comisión Federal de Comercio se encarga de la aplicación de esta ley y de la Normativa sobre Ventas por Teléfono[234/], que prohíbe el abuso y las prácticas engañosas de telemercadeo. La Comisión Federal de Comercio está facultada para iniciar procesos en los tribunales de distrito por infracciones a la Ley de la propia comisión o a la Normativa sobre Ventas por Teléfono, y procurar la reparación justa por los daños, según corresponda a cada caso, incluida la rescisión o modificación de contratos, la restitución, el reembolso de cantidades pagadas y la restitución de ganancias mal habidas.[235/] Generalmente, cuando se procuran sanciones administrativas por infracciones a la Normativa sobre Ventas por Teléfono, el caso es llevado en representación de la Comisión Federal de Comercio.

---

229. 15 U.S.C. §§ 1681n, 1681o
230. 15 U.S.C. § 1681q
231. 15 U.S.C. § 1681s(a)
232. 15 U.S.C. § 6805
233. 15 U.S.C. §§ 6101-6108
234. 16 C.F.R. Parte 310
235. 15 U.S.C. §§ 53(b), 57b, 6102(c), y 6105(b)

Ley de Control del Ataque por Pornografía y Mercadeo No Solicitado. Tanto la Comisión Federal de Comercio como la Comisión Federal de Comunicaciones comparten responsabilidades en estas disposiciones. La Comisión Federal de Comunicaciones puede aplicar las restricciones de la Comisión Federal de Comercio sobre cualquier mensaje de correo electrónico de carácter comercial enviado a un dispositivo alámbrico, por ejemplo una computadora de escritorio, si el remitente es una empresa de comunicaciones (teléfono, radio, radiolocalizador, cable o televisión) o el mensaje anuncia o promueve un producto o servicio de una compañía de comunicaciones.[236/]

La Comisión Federal de Comunicaciones tiene sus propias leyes reglas y una entidad encargada de implementarlas conforme a la Ley de Control del Ataque por Pornografía y Mercadeo No Solicitado, en particular en lo que se refiere a los "mensajes comerciales en servicios móviles", es decir, mensajes de correo electrónico comerciales que son transmitidos directamente a un dispositivo inalámbrico. Entre otras cosas, este tipo de mensajes no pueden ser enviados sin el consentimiento previo y expreso del destinatario, y los remitentes deben dejar de enviarlos en un plazo de 10 días si así lo solicita el destinatario.[237/]

La Ley de Control del Ataque por Pornografía y Mercadeo No Solicitado tiene como objetivo hacer innecesarias –o reemplazar– las leyes estatales contra el correo basura, pero los Estados están autorizados a aplicar la parte de esta ley correspondiente al correo basura dirigido a aparatos alámbricos. Asimismo, permanecen vigentes las leyes estatales que prohíben cualquier acto fraudulento o engañoso y los delitos cibernéticos.

Ley de Portabilidad y Responsabilidad de Seguros Médicos. La Ley de Portabilidad y Responsabilidad de Seguros Médicos (Ley HIPAA), enmendada conforme a la Ley de Tecnologías de la Información en la Salud para el Bienestar Económico y Clínico (Ley HITECH), faculta al Departamento de Salud y Servicios Humanos a imponer sanciones administrativas escalonadas por infracciones al reglamento, según el grado de culpabilidad. Estas sanciones van desde US$100 a US$50.000 o más por infracción, con un límite de US$1,5 millones por año civil en caso de infracciones similares. La Ley HIPAA también faculta al Departamento de Justicia para imponer sanciones penales. Además, la Ley HITECH confirió a los fiscales estatales la autoridad para implementar las protecciones dispuestas en la Ley HIPAA incoando acciones civiles en representación de los residentes de un determinado Estado por infracciones a la Ley HIPAA. Los fiscales estatales están autorizados para procurar la imposición de medidas cautelares o el pago de daños hasta por US$100.00 por infracción, con un límite de US$25.000 por año civil en caso de infracciones similares.

Política federal para la protección de sujetos humanos. En la sección [289/] de la Ley de Servicios de Salud Pública se autoriza a la Oficina para la Protección de Seres Humanos en Investigaciones para que, en representación del Departamento de Salud y Servicios Humanos, establezca un proceso de vigilancia para los casos de violaciones a los derechos de seres humanos sujetos de investigaciones llevadas a cabo o patrocinadas por el Departamento de Salud y Servicios Humanos. Conforme a lo anterior, el Departamento de Salud y Servicios Humanos puede recibir informes de este tipo de violaciones y emprender las medidas que considere pertinentes.

---

236. *Véase* el sitio web de la Comisión Federal de Comunicaciones http://www.fcc.gov/guides/spam-unwanted-text-messages-and-email

237. *Véase* 47 C.F.R. § 64.3100.

Ley Estadounidenses con Discapacidades. La Ley de Estadounidenses con Discapacidades puede ser invocada por la Comisión para la Igualdad de Oportunidades en el Empleo (la cual ha creado recursos administrativos), por el Procurador General de Estados Unidos en los tribunales federales o por cualquier persona que alegue haber sido objeto de discriminación por motivo de alguna discapacidad, del mismo modo que conforme a la sección VII de la Ley de Derechos Civiles de 1964.[238/]

Ley de Comunicaciones. Según la Ley de Comunicaciones, una persona cuyos derechos de privacidad han sido violentados por una empresa de telecomunicaciones puede presentar una denuncia ante la Comisión Federal de Comunicaciones[239/] o puede demandar el pago de daños ante un tribunal federal[240/], pero no puede hacer uso de ambos recursos.[241/] La Comisión Federal de Comunicaciones está facultada tanto para emitir requerimientos contra compañías de telecomunicaciones por infracciones a la Ley de Comunicaciones como multarlos por ignorar tales requerimientos.[242/] Una persona cuyos derechos de privacidad han sido vulnerados por un operador de cable o satélite puede presentar una denuncia ante la Comisión Federal de Comunicaciones o procurar el pago por daños ante los tribunales federales.[243/] Asimismo, cualquier persona que reciba una llamada telefónica, un fax o un mensaje de correo electrónico de naturaleza comercial en un dispositivo inalámbrico, sin haberlo solicitado, puede presentar una denuncia ante la Comisión Federal de Comunicaciones o procurar el pago por daños ante los tribunales estatales y federales.[244/]

Cualquier persona que de manera consciente y deliberada infrinja las disposiciones de la Ley de Comunicaciones[245/] o intercepte y publique comunicaciones hechas por cable o radio estará sujeta a posibles multas o penas de cárcel.[246/] Aquella persona que consciente y deliberadamente transgreda el reglamento de la Ley de Comunicaciones también estará sujeta a multas.[247/] Por último, cualquier persona que de manera consciente y repetida no cumpla con lo dispuesto en la Ley de Comunicaciones o cualquier reglamento emitido por la Comisión Federal de Comunicaciones puede estar sujeta a penas administrativas.[248/]

Además, según se indicó anteriormente, la Comisión Federal de Comunicaciones puede ejercer directamente sus potestades contra aquellas personas que infrinjan la Ley de Comunicaciones o los reglamentos de la misma y puede imponer penas administrativas.[249/] Ley de Privacidad en Comunicaciones Electrónicas dispone penas de carácter civil. Los tribunales pueden conceder indemnizaciones por daños, así como honorarios y costos por los servicios de un abogado.

---

238. Sección 12117 (Ley Estadounidenses con Discapacidades, sección 107).
239. 47 U.S.C. § 208
240. 47 U.S.C. §§ 206
241. 47 U.S.C. § 207
242. 47 U.S.C. § 205
243. 47 U.S.C. §§ 338(i)(7), 551(f)
244. 47 U.S.C. § 227
245. 47 U.S.C. § 501
246. 47 U.S.C. § 605(e)
247. 47 U.S.C. § 502
248. 47 U.S.C. § 503
249. 47 U.S.C. § 503

Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad.[250/] Esta ley es administrada por la Oficina para el Cumplimiento de los Derechos de las Familias en el Departamento de Educación[251/], y se encarga de investigar las supuestas violaciones a los estatutos y reglamentos y proporciona asistencia técnica a las entidades e instituciones educativas sobre el cumplimiento de la ley. En la Ley de Disposiciones Generales en materia de Educación, el Congreso otorgó al Secretario la facultad y discreción para emprender las acciones que considere pertinentes contra cualquier entidad receptora de fondos de cualquier programa administrado por el Secretario, por el incumplimiento de cualquier disposición de la ley aplicable, incluida la Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad.[252/] Los métodos de aplicación previstos en la Ley de Disposiciones Generales en materia de Educación permiten expresamente al Secretario ordenar a la parte infractora que cese y desista de sus acciones, ordenar la recuperación de fondos enviados individualmente, la retención de pagos futuros, forzar el cumplimiento de un acuerdo o "tomar cualquier medida permitida por la ley", incluso entablar una demanda para el cumplimiento de lo dispuesto en la Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad.[253/] El Secretario puede utilizar una o varias de estas medidas según lo considere pertinente dadas las circunstancias. Además, el Departamento está facultado para imponer la regla de los cinco años contra cualquier entidad que la Oficina para el Cumplimiento de los Derechos de las Familias determine que ha infringido la Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad, ya sea mediante la divulgación indebida de información personal identificable derivada de expedientes escolares o por no haber destruido dicha información.

Enmienda sobre la Protección de los Derechos de los Alumnos.[254/] Esta enmienda también es administrada por la Oficina para el Cumplimiento de los Derechos de las Familias en el Departamento de Educación. La enmienda no dispone derechos de acción, pero en caso de violaciones a ésta se aplican las mismas disposiciones de la Ley de Disposiciones Generales en materia de Educación válidas para la Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad. Ni la Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad ni la Enmienda sobre la Protección de los Derechos de los Alumnos disponen el derecho particular a entablar acciones para tutelar un derecho sustantivo.[255/]

Ley de Protección del Consumidor de Servicios Telefónicos. Según esta ley, una persona o entidad puede, en un tribunal estatal pertinente si lo permiten las leyes o reglamentos del Estado de

---

250. Sección 444 de la Ley de Disposiciones Generales en materia de Educación, conocida generalmente como la Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad, 20 U.S.C. § 1232g; 34 CFR parte 99.

251. *Véase* el sitio web del Departamento de Educación en http://www2.ed.gov/policy/gen/guid/fpco/index.html.

252. 20 U.S.C. § 1234c(a).

253. 20 U.S.C. 1234a, 1234c(a), 1234d; 1234e; 1234f; 34 CFR 99.67(a); *véase* también United States v. Miami Univ., 294 F.3d 797 (6th Cir. 2002) (en el que se afirma la decisión del tribunal de distrito de que Estados Unidos puede entablar una demanda para hacer que se respete la Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad).

254. Ley de Disposiciones Generales en materia de Educación, sección 445, conocida generalmente como Enmienda sobre la Protección de los Derechos de los Alumnos, 20 U.S.C. § 1232h; 34 CFR parte 98.

255. En el caso *Gonzaga University v. John Doe*, 526 U.S. 273 (2002), la Corte Suprema de Estados Unidos determinó que, según 42 U.S.C. § 1983, ni los estudiantes y los padres pueden demandar por el pago de daños para hacer valer las disposiciones de la Ley sobre los Derechos de la Familia en Materia de Educación y Privacidad.

que se trate, demandar al infractor de esta ley para que desista judicialmente la realización de tales infracciones o para que pague una indemnización por daños.[256/]

Ley de Protección de la Privacidad de los Conductores. Esta ley dispone sanciones penales y administrativas, y puede ser invocada tanto por las autoridades federales como por individuos.[257/]

Por lo general se disponen de recursos judiciales para los hechos que justifican una acción por actos ilícitos en materia de privacidad, pero varían de un estado a otro. [258/] Además, los 50 estados tienen leyes diversas sobre privacidad/protección de datos en las siguientes áreas, y también disponen recursos y acciones específicas: 1) acceso por parte del paciente a sus expedientes médicos[259/]; 2) restricciones sobre la divulgación de expedientes médicos identificables[260/]; 3) reglas sobre el privilegio de confidencialidad de expedientes de comunicaciones entre pacientes y profesionales de la salud, incluidos los profesionales de salud mental[261/]; y 4) leyes específicas sobre ciertas enfermedades. Cada categoría de ley tiene sus propios recursos, penas y multas específicas para cada Estado.[262/]

---

256. *Véase* 47 U.S.C. §§ 227(b)(3), (c)(5).
257. 18 U.S.C. §§ 2723, 2724.
258. *Véase* Privacilla, How U.S. State Law Quietly Leads the Way in Privacy Protection, Julio de 2002, en http://www.privacilla.org/releases/Torts_Report.pdf.
259. No todos los estados tienen estatutos específicos mediante los que se otorgan a los pacientes el derecho a tener acceso a sus expedientes médicos. Por ejemplo, en Arizona los proveedores de servicios médicos deben dar a los pacientes acceso a sus expedientes médicos y solo existen unos cuantos motivos para negarles el acceso, por ejemplo, para proteger la salud, seguridad o información de otra persona [Ariz. Rev. Stat. § 12-2293]. Otros Estados no tienen leyes específicas sobre esta materia.
260. Pueden ser varias las entidades que restrinjan la divulgación de expedientes médicos identificables, como es el caso de las organizaciones dedicadas al mantenimiento de la salud [Neb. Rev. Stat. §§ 44-32,172, 44-7210], entidades de cuidados administrados [Idaho Code § 41-3930(d)], farmacólogos [Idaho Code § 54-1727], médicos [Idaho Code § 54-1814(13)], asistentes de médicos [Ariz. Rev. Stat. §§ 12-2292, 12-2291], gobiernos estatales [Idaho Code § 9-340C(13)] y agentes revisores [Ala. Code § 27-3A-5(a)(7)], etc. Por lo general, se requiere el consentimiento por escrito del paciente para divulgar la información, a no ser que así lo dispongan las leyes de otros Estados.
261. Algunos Estados reconocen diversos privilegios, en trámites jurídicos, que permiten a los pacientes negarse a dar a conocer su información o que impiden a otros divulgar comunicaciones confidenciales intercambiadas con un profesional para la realización de un diagnóstico y un tratamiento. Entre los estatutos de Arizona se incluyen los siguientes: [Ariz. Rev. Stat. §§ 12-2235 (médico o cirujano-paciente); 13-4430 (asesor-víctima de un delito); 32-2085 (psicólogo-paciente) y 32-3283 (profesional de salud mental-cliente)].
262. Leyes específicas. Algunos estados tienen registros de pacientes con enfermedades específicas, tales como el cáncer [Ala. Code §§ 22-13-33; 22-13-34; 36-12-40] y defectos de nacimiento [Alaska Administrative Code 7 AAC 27.012; Delaware Administrative code Title 16 § 4101] en los que la información de identificación es confidencial, privilegiada y no está disponible al público [Alaska Administrative Code 7 AAC 27.890]. Otros Estados requieren que se informe acerca de enfermedades transmisibles y el VIH/SIDA [Ind. Code Ann. § 16-41-2-1], pero protegen la información con la que puede identificarse al paciente y permite su divulgación con el consentimiento de esta persona, con la finalidad de ejecutar las leyes de salud pública o proteger la vida de otra persona identificada [Ind. Code Ann. § 16-41-8-1(b)]. En el caso de algunos trastornos mentales, algunos Estados requieren que los médicos consigan el consentimiento por escrito del paciente antes de dar a conocer comunicaciones confidenciales sobre el paciente, incluidos hechos sobre su tratamiento, aunque se

No se dispone de datos sobre los demás estatutos federales y estatales referentes a la privacidad/protección de datos o que pueden hacer referencia a recursos judiciales.

ii. Protección de datos/autoridades ejecutoras

Comisión Federal de Comercio. El ámbito de jurisdicción de la Comisión Federal de Comercio abarca la protección al consumidor y la competencia. Es también una de las primeras entidades encargadas de hacer valer las leyes en materia de privacidad en Estados Unidos. Las áreas de privacidad y seguridad de datos entran dentro del ámbito de su misión como entidad dedicada a la protección del consumidor.

La Comisión Federal de Comercio es una entidad independiente del Gobierno de Estados Unidos encabezada por cinco comisionados, nominados por el Presidente de Estados Unidos y confirmados por el Senado. El Presidente escoge a uno de los comisionados como presidente de la Comisión. No más de tres comisionados pueden ser de un mismo partido político. En virtud de que los comisionados son nominados para períodos escalonados de siete años, suele suceder que los comisionados nombrados por un Presidente concluyan su mandato en el período del Presidente siguiente, independientemente del partido político al que pertenezca dicho Presidente.

Esta Comisión tiene aproximadamente 1100 empleados de tiempo completo. De éstos, aproximadamente 50 abogados, investigadores y tecnólogos dedican prácticamente la mayoría de su tiempo al tema de la privacidad. El presupuesto total de la Comisión Federal de Comercio para el año fiscal 2011 fue de US$292 millones.

En 2011, la Comisión Federal de Comercio recibió más de 1.8 millones de quejas vinculadas a su misión de protección al consumidor. Una parte de ellas se relacionan con el tema de la privacidad y seguridad de datos. Sin embargo, la Comisión Federal de Comercio no atiende cada una de las quejas en forma individual, sino que elige aquellas para las que emprenderá una acción judicial.

Comisión Federal de Comunicaciones. La Comisión Federal de Comunicaciones se encarga de proteger la privacidad y seguridad de la información de los consumidores recabada a través de proveedores de servicios de comunicaciones, poniendo en práctica y monitoreando lo dispuesto en la Ley de Comunicaciones de 1934, enmendada, en materia de privacidad y seguridad. Es una entidad independiente del Gobierno de Estados Unidos encabezada por cinco comisionados, nominados por el Presidente de Estados Unidos y confirmados por el Senado. El Presidente escoge a uno de los comisionados como presidente de la Comisión. Solo tres comisionados pueden ser del mismo partido político en determinado momento y ninguno debe tener un interés económico en ninguna de las actividades relacionadas con la Comisión. Todos los comisionados, incluido su presidente, ocupa su

---

permite la divulgación sin el consentimiento en caso de que el paciente represente un peligro para sí mismo u otros [Mass. Gen. Laws Ch. 112 § 129A]. Otros Estados tienen sistemas de vigilancia de enfermedades crónicas [Ariz. Rev. Stat. § 36-133]. Las pruebas genéticas también están reguladas por los Estados, al no permitir que se utilicen los resultados de tales pruebas para discriminar contra las personas, por ejemplo, en el caso de seguros [Ala. Code §§ 27-53-1, 27-53-2]. Algunos Estados prohíben la divulgación de información relacionada con enfermedades de transmisión sexual, a no ser que sea necesario para evitar su diseminación [Ala. Code §§ 22-11A-14, 22-11A-22 and 22-11A-38].

cargo durante cinco años, salvo cuando son nombrados para cubrir la vacante dejada por otro que no terminó su período. Esta Comisión tiene aproximadamente 1.900 empleados de tiempo completo.

Departamento de Salud y Servicios Humanos. La Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos es responsable de la ejecución en el ámbito civil de la cláusula de privacidad, seguridad y fallas de la Ley HIPAA. Esta oficina tiene aproximadamente 239 empleados encargados de administrar y velar por la implementación de los reglamentos y leyes federales en materia de derechos civiles. Su presupuesto para el año fiscal 2011 ascendió a US$41 millones. La Oficina para la Protección de Seres Humanos en Investigaciones recibe aproximadamente una queja al año por violaciones a las disposiciones en materia de privacidad o protección de datos del Departamento de Salud y Servicios Humanos. Esta oficina tiene potestad para evaluar posibles incumplimientos y tiene discreción para determinar si lleva a cabo una evaluación.

Departamento de Educación. La Oficina para el Cumplimiento de los Derechos de las Familias, del Departamento de Educación, tiene aproximadamente 10 empleados de tiempo completo. Desde abril de 2003 (fecha de cumplimiento) y hasta finales de 2011, el Departamento de Salud y Servicios Humanos había recibido más de 67,000 quejas en materia de privacidad y seguridad, de individuos y otras entidades; de estas más de 23,000 han sido objeto de investigación. Esta oficina recibió cerca de 700 cartas en el último año, las cuales contienen quejas y solicitudes de asistencia técnica.

No se disponen datos de otras autoridades estatales o federales.

iii. Capacidades de investigación/procesamiento penal

Comisión Federal de Comercio. Si esta Comisión a de iniciar alguna investigación, debe basar su decisión en diferentes factores, incluidos la existencia de quejas de los consumidores. Otros factores pueden ser las propias investigaciones que ha llevado a cabo la Comisión, recomendaciones de otras organizaciones del sector privado y de la sociedad civil, compañías de marcas de confianza y organizaciones dedicadas a la defensa de la privacidad; informes de los medios sobre problemas de privacidad nuevos o ya diseminados; las prioridades que determine la propia Comisión; los posibles daños a los consumidores; la necesidad de probar o aplicar nuevas leyes o reglamentos y otras consideraciones importantes. Sin embargo, la Comisión Federal de Comercio no atiende cada una de las quejas en forma individual, sino que elige aquellas para las que emprenderá una acción judicial.

Comisión Federal de Comunicaciones. La Comisión Federal de Comunicaciones decide cuándo ha de iniciar una investigación tomando en cuenta diferentes factores, incluidos la existencia de quejas de los consumidores, investigaciones internas sobre las leyes y hechos relevantes, informes de los medios sobre problemas nuevos o ya diseminados en el sector de las comunicaciones, las prioridades de la propia Comisión y los posibles daños a los consumidores.

Departamento de Salud y Servicios Humanos. Este departamento realiza investigaciones tanto en respuesta a las quejas recibidas como los resultados de las evaluaciones que realiza. Además, este departamento ha instaurado un programa de auditorías a las entidades cubiertas por las disposiciones de la Ley HIPPA.

Oficina para la Protección de Seres Humanos en Investigaciones. Esta oficina lleva a cabo evaluaciones de cumplimiento con y sin motivos fundados, entre los que se pueden incluir cualquier inquietud sobre la privacidad de los sujetos de investigaciones o la confidencialidad de los datos de la investigación. Las evaluaciones de cumplimiento por motivos fundados se llevan a cabo cuando esta oficina recibe por escrito denuncias sustantivas o indicaciones de que no se cumplen las disposiciones del Departamento de Salud y Servicios Humanos. Las evaluaciones sin motivo fundado se llevan a cabo cuando no se cuentan con los alegatos o indicaciones correspondientes. Las instituciones que han de ser objeto de este tipo de evaluaciones son seleccionadas tomando como base diversas consideraciones, incluidas las siguientes: (a) el volumen de investigaciones en las que participan, llevadas a cabo por o con el apoyo del Departamento de Salud y Servicios Humanos; (b) si han presentado pocos informes a la Oficina para la Protección de Seres Humanos en Investigaciones conforme a los reglamentos del Departamento de Salud y Servicios Humanos[263/]; (c) la necesidad de evaluar la implementación de medidas correctivas luego de una evaluación llevada a cabo con motivo fundado; (d) la ubicación geográfica; (e) la certificación por parte de grupos profesionalmente reconocidos de programas para la protección de sujetos humanos, y (f) las evaluaciones y auditorías recientes relativas a la protección de sujetos humanos llevadas a cabo por otras entidades regulatorias (tales como la Administración de Alimentos y Medicamentos) o su participación reciente en programas de mejora de la calidad (tales como el programa de Mejora de la Calidad de la Oficina para la Protección de Seres Humanos en Investigaciones).

Por lo que se refiere a las quejas sujetas a posibles acciones penales, la Ley de Imparcialidad en la Calificación de Crédito dispone sanciones penales por la obtención de informes de consumidores con falsas pretensiones[264/]; la Ley de Privacidad de las Comunicaciones Electrónicas establece que ciertas violaciones conllevan sanciones penales[265/]; la Ley de Comunicaciones dispone que cualquier persona que de manera consciente y deliberada viole una de sus disposiciones puede ser multada o sentenciada a cumplir penas de cárcel[266/], y la Ley HIPPA autoriza al Departamento de Justicia a imponer las sanciones que dispone dicha ley. En este último caso, el Departamento de Salud y Servicios Humanos remite al Departamento de Justicia las quejas para las cuales la Ley HIPPA dispone sanciones penales. A finales de 2011, el Departamento de Salud y Servicios Humanos había remitido 499 posibles violaciones al Departamento de Justicia. El Departamento de Salud y Servicios Humanos puede imponer penas administrativas por violaciones al reglamento de la Ley HPPA , por las que también se disponen sanciones penales.

No se disponen datos de autoridades estatales.

---

263. 45 CFR 46.103(b)(5)

264. 15 U.S.C. § 1681q.

265. 18 U.S.C. § 2511(4). *Véase también* 18 U.S.C. § 3121(d) (sanciones penales por violaciones al estatuto Pen/Trap).

266. 47 U.S.C. § 501.

C. Cooperación transfronteriza

i. Transferencia de datos

Conforme a las leyes de Estados Unidos, no existen restricciones generales a la transferencia de datos a otros países. Sin embargo, las transferencias de datos médicos y de otro tipo relacionados con la salud por parte de organizaciones del sector privado reguladas por la Ley HIPPA deben cumplir con el reglamento correspondiente; por ejemplo, deben ser para un propósito permisible y con las debidas salvaguardas razonables. Además, el intercambio de información y pruebas, incluidos los datos personales, entre autoridades estadounidenses y sus contrapartes extranjeras está sujeto a los requerimientos de confidencialidad estipulados en las leyes, reglamentos, tratados de asistencia jurídica mutua y otros acuerdos de cooperación pertinentes.

ii. Instrumentos/acuerdos internacionales

Estados Unidos ayudó a elaborar y adoptó las Directrices de la OCDE que Rigen la Protección de la Privacidad y el Marco de Privacidad del APEC. Asimismo, Estados Unidos ayudó a elaborar el Sistema de Reglas Transfronterizas sobre Privacidad del APEC y pretende participar en este programa una vez que entre en operación. Este sistema es un programa autorregulatorio que pretende respaldar las acciones de los Gobiernos. Así pues, una vez que entre en operación y que las compañías estadounidenses sujetas a la jurisdicción de la Comisión Federal de Comercio se afilien al programa, esta Comisión aplicará dicho sistema de reglas.

Estados Unidos también ha negociado con la Comisión Europea el Marco de Seguridad Estados Unidos-Unión Europea que satisface requerimientos de “suficiencia” de la Directiva sobre Protección de Datos de la Unión Europea. Las compañías que se afilien a este programa podrán transferir legalmente datos personales de la Unión Europea a Estados Unidos conforme a los principios estipulados en el Marco de Seguridad.

iii. Cooperación transfronteriza en materia de investigación y ejecución de las leyes

Intercambio de información. La Comisión Federal de Comercio tiene amplia experiencia en el campo de la cooperación e intercambio de información con otros países, incluso en casos relacionados con la privacidad. En 2006, la Ley Web Segura otorgó más libertad a la Comisión Federal de Comercio para cooperar con otros países. Entre otras cosas, otorgó a la Comisión la facultad de entregar pruebas a autoridades de otros países como apoyo a sus investigaciones o actividades encaminadas a la ejecución de las leyes.

Las autoridades extranjeras pueden presentar una solicitud para intercambiar información o solicitar ayuda en una investigación conforme a la mencionada ley. Una entidad extranjera se define en esta ley como cualquier entidad o autoridad judicial de un Gobierno extranjero (incluido un Estado, una subdivisión política de este o una entidad multinacional integrada por diversos Estados) con la autoridad en materia civil, penal o administrativa para aplicar las leyes o llevar a cabo investigaciones. Incluye también cualquier organización internacional que actúe en representación de dicha entidad.

La entidad extranjera debe presentar un certificado por escrito en el que conste que los materiales que habrá de recibir serán confidenciales en todo momento y que se utilizarán solamente para propósitos oficiales. Asimismo, debe identificar el fundamento legal de sus potestades para resguardar debidamente el material que habrá de recibir.

La Comisión Federal de Comercio puede compartir información confidencial con entidades extranjeras si ésta habrá de utilizarse para investigar o llevar a cabo procesos legales relacionados con infracciones a leyes de otros países que prohíben prácticas comerciales fraudulentas o engañosas, u otras prácticas que sean sustancialmente similares a las prácticas prohibidas por las leyes que administra la Comisión; las leyes que administra la Comisión, si la divulgación de material favorece las investigaciones o los procedimientos legales; o, con la aprobación del Procurador General de Estados Unidos, cualquier código penal extranjero, si se trata de delitos definidos en un tratado de asistencia jurídica mutua entre Estados Unidos y el país solicitante.

Los criterios anteriores también se aplican a las infracciones relacionadas con la privacidad. Si el asunto está relacionado con un banco, una institución de ahorros y préstamos o una cooperativa de crédito, la Comisión Federal de Comercio debe obtener primero la aprobación del regulador pertinente antes de compartir información.

En el caso de la Comisión Federal de Comercio, la colaboración es tanto informal como formal y con los miembros y no miembros de la red GPEN y del acuerdo CPEA del APEC. La Comisión Federal de Comercio considera que las redes y marcos de cooperación como los indicados anteriormente son invaluables para mejorar la cooperación entre países. Así, la Comisión Federal de Comercio ha participado activamente en el desarrollo tanto de la red GPEN como del acuerdo CPEA del APEC.

Cooperación. Conforme a la Ley Web Segura, la Comisión Federal de Comercio también debe prestar asistencia en investigaciones o procesos legales para casos de infracciones a las leyes que prohíben las prácticas fraudulentas o engañosas, o las prácticas sustancialmente similares a aquellas que prohíben las leyes que administra la Comisión, incluidas las infracciones a la privacidad. La Ley Web Segura excluye las investigaciones o acciones de otros países dirigidas contra bancos, instituciones de ahorro y préstamo, cooperativas de crédito federales y portadores comunes que no entran dentro de la jurisdicción de la Comisión Federal de Comercio.

El principal tipo de ayuda que puede prestar la Comisión Federal de Comercio es el emplazamiento administrativo para la presentación de documentos u otras pruebas. En representación de autoridades extranjeras, la Comisión Federal de Comercio ha obtenido información de diversas compañías, incluso de aquellas dedicadas al registro de dominios, proveedores de servicios de correo electrónico y de servicio telefónico, utilizando este mecanismo. La Comisión Federal de Comercio ha conseguido la información suscriptores y la ha entregado a entidades extranjeras, lo cual les ha ayudado a confirmar la identidad de sospechosos involucrados en fraudes, así como la identidad de otras víctimas de dichos fraudes. La ley autoriza también a la Comisión Federal de Comercio a utilizar otros mecanismos para obtener información en representación de entidades extranjeras.

Para decidir si colabora en una investigación, la Comisión Federal de Comercio debe considerar los siguientes factores: si la entidad solicitante ha convenido o ha manifestado su voluntad de proporcionar ayuda recíproca (no necesariamente en el mismo asunto); si la autorización de la

solicitud afectaría los intereses del público estadounidense, y si la labor de la entidad solicitante podría derivar en actos o prácticas que puedan provocar o que de hecho provoque daños a un número considerable de personas.

D. Jurisprudencia y retos especiales

Los jueces y especialistas en derecho de Estados Unidos han considerado que las protecciones en materia de privacidad dispuestas en la Cuarta Enmienda de la Constitución de Estados Unidos para la protección de objetos y espacios físicos contra registros por parte del Gobierno, van más allá del mero respeto a la seguridad e intimidad indispensables para el bienestar y participación en una sociedad democrática.[267/] Los tribunales han reconocido también que los individuos tienen intereses sustantivos en materia de privacidad contra entidades privadas.[268/]

El derecho consuetudinario –particularmente el derecho de responsabilidad civil en el ámbito estatal– ha desempeñado un papel importante en el desarrollo del marco relativo a la privacidad de datos comerciales en Estados Unidos.[269/] El origen de todo esto se encuentra en el artículo "The Right to Privacy" de Samuel Warren y Louis Brandeis, publicado en 1890. En este artículo sus autores destacaron particularmente el derecho de mantener la información personal fuera del alcance del dominio público. De esta forma, se sentaron las bases para el desarrollo del derecho consuetudinario en materia de privacidad, entendido por algunos como algo más que el "derecho a no ser molestado", incluido el derecho a controlar la información personal en gran parte del siglo XX.[270/]

La rápida evolución de las tecnologías de la información y las prácticas que facilitan estas tecnologías plantean serios retos para todos los regímenes de privacidad. Sin embargo, sería prematuro señalar algunas tecnologías en particular. La tecnología sigue desarrollándose con rapidez y el Gobierno considera que los procesos en los que intervienen diversos factores, tales como los presentados el informe oficial, podrían ser flexibles y podrían ofrecer la mejor solución a los retos que plantea un entorno técnico, económico y social en constante evolución. Esta recomendación

---

267. *Véase, por ejemplo, City of Ontario v. Quon*, 130 S.Ct. 2619, 2627 (2010) ("La [Cuarta] Enmienda garantiza la privacidad, dignidad y seguridad de las personas contra determinados actos arbitrarios e invasivos de funcionarios del gobierno.") (citas omitidas); *Kyllo v. United States*, 533 U.S. 27, 31 ("La esencia misma de la Cuarta Enmienda es el derecho del hombre a refugiarse en su propio hogar y así apartarse de cualquier intromisión irrazonable por parte del Gobierno.") (cita interna omitida); *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., discrepa) ("[Los autores de la Constitución] pretendían proteger a los estadounidenses en sus creencias, pensamientos, emociones y sensaciones. A diferencia del Gobierno, les confirieron el derecho a que los dejaran en paz: el derecho más amplio de mayor valor para los hombres civilizados.")
268. *Véase Mainstream Marketing Services., Inc. v. FTC*, 358 F.3d 1228, 1232-33 (10th Cir. 2004) (establece que la defensa de la privacidad del consumidor es importante para el Gobierno y que el restringir las llamadas de telemercadeo protege este interés y no va en contra de la Primera Enmienda).
269. *Véase* Privacilla, How U.S. State Law Quietly Leads the Way in Privacy Protection, julio de 2002, en http://www.privacilla.org/releases/Torts_Report.pdf.
270. Sin embargo, no todos los tribunales y especialistas han considerado la privacidad como el "derecho a no ser molestado". Dean William Prosser examinó diversos casos de privacidad en el derecho consuetudinario y llegó a postular que el ejercicio del derecho a la privacidad se limita a cuatro circunstancias: la intrusión en la intimidad, la divulgación de hechos privados, la presentación de una imagen tergiversada de una persona y el adueñarse de su nombre o imagen. *Véase* William L. Prosser, Privacy, 48 CALIFORNIA LAW REVIEW 383, 389 (1960).

refleja la opinión de que el Gobierno debe apoyar el desarrollo de políticas que sean lo suficientemente simplificadas para responder con rapidez ante problemas de privacidad de datos de consumidores y que incorporen las perspectivas de todas las partes interesadas de la mejor manera posible. Un proceso en el que se tomen en cuenta debidamente a todas las partes interesadas permitirá atender los problemas con nuevas tecnologías y métodos de trabajo sin necesidad de requerir más leyes; permitirá a las partes interesadas reevaluar con rapidez las cambiantes expectativas de los consumidores, y permitirá a las partes interesadas identificar los riesgos en las primeras etapas del desarrollo de nuevos productos y servicios.

El hecho de que los flujos de datos abarque cada vez más países complica nuestros retos pues ello requiere el desarrollo de regímenes de privacidad que no solo puedan ajustarse a los constantes cambios en la tecnología y métodos de trabajo, sino que también permitan la interoperabilidad y la cooperación entre diferentes jurisdicciones con distintos regímenes jurídicos. Entre los ejemplos recientes de intentos por crear esquemas flexibles de interoperabilidad transfronteriza puede mencionarse el Sistema de Reglas Transfronterizas sobre Privacidad del APEC, que es un programa de privacidad negociado, multilateral y autorregulatorio para empresas, y que es respaldado por las autoridades.

11. Uruguay