Estudio sobre Protección de Datos a nivel internacional

Noviembre 2004

INDICE

0. INTRODUCCIÓN

El presente Informe, realizado en interés del Instituto Federal de Acceso a la Información Pública Gubernamental (en adelante, IFAI) refleja el análisis y estudio en materia de protección de datos de carácter personal en las legislaciones que sobre la materia regulan los países de Argentina, Canadá, España y México. Se trata, por tanto, de llevar a cabo una comparativa a nivel internacional en la materia que permita ofrecer alternativas a tomar en consideración para establecer una regulación sobre este tema en México.

La estructura conforme a la cual se va a desarrollar este Informe es la de considerar la regulación que de la protección de datos de carácter personal realiza, de un lado, el Convenio (108) del Consejo de Europa, para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, de 28 de enero de 1981 y la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y, de otro lado, las legislaciones que, como pretende realizar México, establecieron la regulación en su día de la Protección de Datos al amparo, en particular, de la citada Directiva europea, como es el caso de la normativa española, o que han sido reconocidas como legislaciones que proporcionan un nivel adecuado de protección a los datos personales y a las que la Unión Europea ha otorgado el reconocimiento de un nivel adecuado de protección de datos al cumplir los requisitos previstos en la Directiva para el mismo, siendo éstas en concreto Argentina y Canadá. Tras analizar esto pasaremos a considerar la normativa que México tiene prevista o pretende prever en la materia[1].

De este modo, en cada apartado del Informe haremos referencia a lo previsto en el Convenio 108 del Consejo de Europa y en la Directiva 95/46/CE, para pasar a continuación a comprobar mediante tablas su puesta en práctica por la legislación de España, Argentina y Canadá y, en último lugar, se analizará las disposiciones correspondientes de la legislación de México.

[1] En este sentido, se incluye el análisis de los Lineamientos para la Protección de los Datos Personales como acercamiento a la posible regulación que establezca sobre la materia.

En concreto, las disposiciones que se analizan a lo largo del presente Informe son las que a continuación, junto con su abreviatura, se reflejan en la tabla.

EUROPA	
Norma	**Abreviatura**
Convenio (108) del Consejo de Europa, para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, de 28 de enero de 1981, firmado en Estrasburgo por el Plenipotenciario de España el 28 de enero de 1982, ratificado mediante Instrumento de 27 de enero de 1984[2].	Convenio 108
Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[3].	Directiva 95/46/CE
ARGENTINA	
Ley Nº 25326. Protección de los Datos Personales.	Ley Nº 25326
Decreto 1558/2001 por el que se aprueba el Reglamento de la Ley.	Reglamento argentino
CANADÁ	
Personal Information Protection and Electronic Documents Act. 13th April, 2000[4]	PIPED Act
ESPAÑA	
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[5].	LOPD
Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal[6].	R.D. 1332/94 o Reglamento español

[2] Publicado en el Boletín Oficial del Estado núm. 274, de 15 de septiembre de 1985.
[3] Publicada en el Diario Oficial de las Comunidades Europeas, L 281, 23/11/1995.
[4] Con el fin de no introducir ninguna alteración en su interpretación se mantiene la versión en inglés de la Ley canadiense.
[5] Publicada en el Boletín Oficial del Estado núm 298, 14/12/1999.
[6] Este Real Decreto fue publicado en el Boletín Oficial del Estado núm. 147, 21/6/1994. Aunque desarrollaba la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD), actualmente derogada por la LOPD, sigue en vigor en virtud de la Disposición Transitoria Tercera de la LOPD. En este sentido, cualquier referencia que se realice a la LORTAD ha de entenderse realizada a la vigente LOPD.

MÉXICO	
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de 11 de junio de 2002	LAI
Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de X de junio de 2003	Reglamento de la LAI
Lineamientos para la Protección de los Datos Personales[7]	Lineamientos

1. ¿Qué es la protección de datos?

Hoy en día es necesaria la utilización de los sistemas de información para poder dar tratamiento al gran volumen de datos que se manejan en todas las actividades tanto públicas como privadas, pero, al mismo tiempo, existe el derecho del titular del dato en lo que se denomina la "autodeterminación informativa"; de esta forma quien tenga, mantenga, utilice o trate, en soporte informático, o en forma automatizada o susceptible de tratamiento automatizado, sistemas de datos de carácter personal -o solamente consulte datos, en forma automatizada, o telemática, a un sistema de datos de un tercero-, se encuentra sometido a la normativa conocida como "protección de datos" que, defiende la llamada "privacidad" de los ciudadanos, con un órgano de control del cumplimiento de la ley. El derecho a la "autodeterminación informativa" supone que el interesado cuyos datos son objeto de tratamiento puede decidir quién, cuándo y cómo se van a tratar sus datos personales. En las modernas legislaciones sobre protección de datos, esta protección se extiende a los tratamientos no automatizados, si bien, la potencial agresividad para la privacidad es mayor en el caso de la utilización de las Tecnologías de la Información y las Comunicaciones (TIC) en el tratamiento de datos de carácter personal, tal y como veremos a lo largo de este Informe.

Pero, ¿qué se entiende por protección de datos?. Siguiendo al Prof. Dr. D. Miguel Ángel Davara Rodríguez entenderemos por protección de datos *"el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado,*

[7] Estos Lineamientos son todavía un Proyecto, si bien los tendremos en consideración a lo largo de nuestro informe. Además, debe tenerse en consideración que ya se han publicado los siguientes: Lineamientos generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal, publicados en el Diario Oficial de la Federación de 18 de agosto de 2003; Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales, publicados en el Diario Oficial de la Federación de 20 de agosto de 2003; Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos, publicados en el Diario Oficial de la Federación de 25 de agosto de 2003, y Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal, en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares, publicados en Diario Oficial de la Federación de 6 de abril de 2004.

para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad".

Con la protección de datos, el derecho que se trata de proteger no es solamente el de la intimidad, sino algo con mayor profundidad que, en los ordenamientos de ámbito anglosajón, se ha dado en llamar *"privacy"* y que nosotros hemos castellanizado como "privacidad".

La protección se realiza sobre el dato, de manera que éste no pueda ser tratado o elaborado, y convertido en información, nada más que para aquellos fines y por aquellas personas autorizadas para ello. Esta necesaria protección es un límite a la utilización de la informática ante el temor de que pueda agredir la intimidad de los ciudadanos, personal o familiarmente, y que pueda coartar el ejercicio de sus derechos.

En principio, no se puede tratar ningún dato de carácter personal sin el consentimiento de su titular o interesado. Por tanto se podrán tratar todos aquellos datos para los que el titular de los mismos haya prestado su consentimiento, salvo que concurra alguna excepción prevista en la Ley a esta necesidad de consentimiento.

Es por tanto el titular de los datos el único que, como norma general, puede decidir cuándo, dónde, cómo y por quién se tratan sus datos de carácter personal.

Una vez indicado qué datos se pueden tratar, diremos en qué forma se deben tratar.

Los datos se deben tratar en la forma que queda especificada en los principios de protección de datos y facilitar el ejercicio de los derechos de los ciudadanos.

Esto es, no es suficiente contar con el consentimiento del titular del dato para poder proceder a su tratamiento, sino que, además, hay que adecuar ese tratamiento al respeto de los principios contemplados en la norma y a facilitar el ejercicio de los derechos por el ciudadano. Así, cabe estructurar el análisis y estudio de la Protección de Datos, siguiendo al Profesor Davara, como un triángulo en cuyos vértices se sitúan los principios de dicha protección, los derechos que emanan de dichos principios y los procedimientos que garantizan el ejercicio efectivo de dichos derechos.

Por último, el tratamiento de los datos de carácter personal ceñido al cumplimiento de los principios y facilitar el ejercicio de los derechos por el titular de los datos, no tendría sentido o, más bien, carecería de aplicación práctica efectiva sin la previsión de unos procedimientos a través de los cuales, por un lado, se pueda garantizarse la tutela de los derechos reconocidos a todo ciudadano y, por otro, se sancione a quienes vulneren la normativa sobre protección de datos.

2. La regulación de la protección de datos en México

Al referirnos a la regulación de la protección de datos de carácter personal, es necesario partir de los diferentes puntos de vista que se plantean en los ordenamientos jurídicos europeo y anglosajón, entiendo hecha la referencia en este último caso a los Estados Unidos (EE.UU.).

Así, en el caso de la Unión Europa, tal y como puede comprobarse en la Directiva 95/46/CE y en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[8], se parte del concepto de sistema de protección de datos señalándose en el considerando 1 del Reglamento (CE) nº 45/2001 que un sistema completo de protección de datos se integra por los siguientes aspectos:

- derechos de las personas;
- obligaciones de quienes tratan los datos personales;
- establecimiento de sanciones apropiadas para los infractores, y
- un organismo de supervisión independiente (al que suele denominarse Autoridad o Agencia de Protección de Datos).

[8] Publicado en el Diario Oficial núm. L 8, de 12 de enero.

En Europa, la regulación de la protección de datos de carácter personal se caracteriza por su previsión en una norma legal respaldada por la previsión de sanciones para los casos en que se produzca un incumplimiento por quien trata los datos de carácter personal por cualquier título, ya sea un responsable del sistema de datos o un encargado del tratamiento.

Por otra parte, el modelo anglosajón se basa en la práctica ausencia de previsiones legales, quedando dicha regulación reducida al establecimiento de códigos de conducta o, la denominada, "autorregulación industrial" desarrollada esencialmente por el sector privado, y cuya efectividad depende, en gran parte, del poder de coacción de quien formula dichos códigos y de la aplicación de las sanciones previstas en ellos.

Por último, y antes de entrar a analizar cada uno de los aspectos que deben tenerse en consideración para establecer un sistema de protección de datos, y en particular en lo que respecta a México, es necesario analizar cuál es la situación actual en dicho país. En este sentido, hay partir del hecho de que en México no hay una ley específica, ni a nivel federal ni a nivel estatal, que regule en sí la protección de datos personales. La primera referencia que se encuentra en el ordenamiento jurídico y el fundamento legal de cualquier norma que vaya a regular posteriormente la protección de datos personales está en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos[9] que establece que *"nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones"*.

No obstante, debe atenderse a la regulación que de la protección de datos personales hace la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (en adelante, LAI), que, si bien es una norma cuyo objeto es, según dispone su artículo 1, *"garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal"*, incide directamente en la privacidad de los individuos cuyos datos personales son objeto de tratamiento, al constituir un límite al acceso a la información. Por tanto, el fundamento constitucional de esta Ley no está en el artículo 16 sino en el 6 que prevé el derecho de acceso a la información en poder de la Administración Pública Federal por parte de los ciudadanos. El desarrollo de la LAI se llevó a cabo mediante el Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

[9] Promulgada el 17 de febrero de 1917.

No obstante, existen iniciativas de ley para regular la protección de datos personales en México, como por ejemplo la propuesta del Comité de Modernización Financiera, que ha presentado un proyecto de Ley de Protección de Datos que abarcaría tanto al sector público como al privado y que regularía el tratamiento de datos personales (manejo, administración, distribución y comercialización) por las sociedades de información.

En definitiva, la necesidad y oportunidad de establecer una regulación específica sobre la protección de datos personales en México está más que justificada desde diversos puntos de vista, entre los que puede destacarse, en primer lugar, la garantía de un derecho de los ciudadanos como es el derecho a la privacidad y, en segundo lugar, los beneficios que ello reporta tanto al sector privado como al público, en cuanto que esta garantía, en caso de que cumpla con unos determinados requisitos, determina que se facilite la realización de transacciones comerciales y de otro tipo con la Unión Europea, buscando así además el reconocimiento de un nivel adecuado por parte de la Comisión Europea, lo que supondría la libre realización de transferencias internacionales de datos con destino a México, como veremos cuentan ya países como Canadá o Argentina.

1. GENERALIDADES

1.1. Objeto

El objetivo del presente apartado es centrar la materia que va a ser analizada a lo largo de este Informe, siendo para ello conveniente partir del objeto de las normas que son motivo de análisis y que exponemos a continuación.

❑ **Convenio (108) del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal** (en adelante, Convenio 108):

> *"El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)"* (art. 1).

❑ **La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta la tratamiento de datos personales y a la libre circulación de estos datos** (en adelante, Directiva 95/46/CE), dispone como objeto de la regulación que acomete el de que:

> *"1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.*
>
> *2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1"* (art. 1).

Por su parte, y con el ánimo de comprobar el objeto de la regulación de la normativa que sobre protección de datos existe en España, Argentina y Canadá, vamos a exponer a través de la siguiente tabla sus disposiciones contenidas en las normas que se indican a continuación:

- Respecto a España, esta materia viene regulada por la **Ley Orgánica15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal** (en adelante, LOPD)[10].

- En cuanto a Argentina, la regulación de la protección de datos la realiza la **Ley Nº 25326 de Protección de los Datos Personales** (en adelante Ley, nº 25326[11]).

- Por último, Canadá tiene regulada esta materia en la Ley ***"Personal Information Protection and Electronic Documents Act"*** de 13 de abril de 2000 (en lo sucesivo, PIPED Act).

En la siguiente tabla se efectúa un análisis comparativo del objeto de las tres normas de referencia:

LOPD	Ley nº 25326	PIPED Act
OBJETO		
Art. 1	**Art. 1**	**1.**
La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar	La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar	The purpose is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances

[10] En materia de Protección de Datos en España, junto a la LOPD deben considerarse subsistentes, conforme a su Disposición Transitoria tercera, el Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (en adelante, R.D.1332/94), y el Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, en lo que no se opongan a la LOPD. Además, es necesario atender a otras normas que regulan determinados aspectos de la protección de datos, así como las Instrucciones de la AEPD.

[11] Determinados aspectos de la Ley se encuentran desarrollados por el Decreto 1558/2001 por el que se aprueba el Reglamento de la Ley.

	las bases de datos ni las fuentes de información periodísticas.	

Entre los objetos de la LAI, destacamos el referente a la protección de datos en el apartado III del artículo 4 que dispone:

> *"Son objetivos de esta Ley:*
> *...*
> *Garantizar la protección de los datos personales en posesión de los sujetos obligados."*

Por su parte los Lineamientos del IFAI sobre protección de datos recogen como objeto de su regulación:

> *"Los presentes Lineamientos tienen por objeto establecer las bases que deberán observar las dependencias y entidades de la Administración Pública Federal para protección de los datos personales recabados en soporte físico, electrónico o que por cualquier circunstancia mantengan en su posesión, sean susceptibles de tratamiento o no."* (art. 1º)

Conclusiones: analizado el objeto de cada una de las normas que son objeto de estudio en este Informe, es necesario tener en consideración que tanto el Convenio 108, como la Directiva 95/46/CE, la LOPD, la Ley argentina y la PIPED Act tienen por objeto regular el tratamiento de los datos de carácter personal llevados a cabo, mientras que la LAI no es una norma legal cuyo objeto sea la regulación de esta materia, sino que la referencia a la protección de datos surge como consecuencia de permitir el acceso a la información pública que maneja la Administración Pública Federal (APF).

A efectos de desarrollar una norma que regule la protección de datos de carácter personal, el legislador debe tener en consideración que su objeto será, precisamente, garantizar el derecho a la privacidad de los ciudadanos, o como también se les denomina en ocasiones "interesados", "afectados" o "titulares de los datos", siendo este derecho una concreción del derecho a la intimidad.

Además, el derecho a la protección de datos personales es un derecho fundamental, al menos en la Unión Europea y es así reconocido por los ordenamientos jurídicos de diversos Estados miembros.

1.2. Ámbito de aplicación

Analizado el objeto de las distintas normas que son motivo de estudio en el presente Informe, procedemos a atender a cuál es el ámbito de aplicación de cada una de ellas.

En el Convenio 108:

En el artículo 3 indica que:

"1. Las partes se comprometen a aplicar el presente Convenio a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado.

2. Cualquier Estado podrá en el momento de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, o en cualquier otro momento ulterior- hacer saber mediante declaración dirigida al Secretario general del Consejo de Europa:

a) Que no aplicará el presente Convenio a determinadas categorías de ficheros automáticos de datos de carácter personal, una lista de las cuales quedará depositada. No deberá sin embargo incluir en esa lista categorías de ficheros automatizados sometidas, con arreglo a su derecho interno, a disposiciones de protección de datos. Deberá, por tanto, modificar dicha lista mediante una nueva declaración cuando estén sometidas a su régimen de protección de datos categorías suplementarias de ficheros automatizados de datos de carácter personal;
b) que aplicará el presente Convenio, asimismo, a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica;
c) que aplicará el presente Convenio, asimismo, a los ficheros de datos de carácter personal que no sean objeto de tratamientos automatizados.

3. Cualquier Estado que haya ampliado el campo de aplicación del presente Convenio mediante una de las declaraciones a que se refieren los apartados 2, b) o c), que anteceden podrá, en dicha declaración, indicar que las ampliaciones solamente se aplicarán a determinadas categorías de ficheros de carácter personal cuya lista quedará depositada.

4. Cualquier parte que haya excluido determinadas categorías de ficheros automatizados de datos de carácter personal mediante la declaración prevista en el apartado 2, a), anterior no podrá pretender que una Parte que no las haya excluido aplique el presente Convenio a dichas categorías.

5. Igualmente, una Parte que no haya procedido a una u otra de las ampliaciones previstas en los párrafos 2, b) y c), del presente artículo no podrá pretender que se aplique el presente Convenio en esos puntos con respecto a una parte que haya procedido a dichas aplicaciones.

6. Las declaraciones previstas en el párrafo 2 del presente artículo tendrán efecto en el momento de la entrada en vigor del Convenio con respecto al Estado que las haya formulado, si dicho Estado las ha hecho en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, o tres meses después de su recepción por el Secretario general del Consejo de Europa si se han formulado en un momento ulterior. Dichas declaraciones podrán retirarse en su totalidad o en parte mediante notificación dirigida al Secretario general del Consejo de Europa. La retirada tendrá efecto tres meses después de la fecha de recepción de dicha notificación."

En la Directiva 95/46/CE:

Las disposiciones de la Directiva 95/46/CE se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un sistema de datos personales (art. 3).

Según se establece en el apartado 2 del artículo 3, las disposiciones de esta Directiva no se aplicarán al tratamiento de datos personales:

a) efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los Títulos V (también conocido como "segundo pilar", contiene disposiciones sobre la Política Exterior y de Seguridad Común) y VI (también conocido como "tercer pilar", contiene disposiciones sobre el establecimiento de una cooperación en los ámbitos de Justicia y Asuntos de Interior) del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;
b) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la Directiva a todo tratamiento de datos personales cuando:

a. el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar

las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b. el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;
c. el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea[12].

En las normas nacionales:

LOPD	LEY Nº 25326.	PIPED Act
ÁMBITO DE APLICACIÓN		
Art. 2	**Art. 44**	**4**
1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal: a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento. b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público. c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.	Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional. Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.	This Part applies to every organization in respect of personal information that (a) the organization collects, uses or discloses in the course of commercial activities; or (b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business. This Part does not apply to (a) any government institution to which the Privacy Act applies; (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or (c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose. Every provision of this Part

[12] En este caso, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas. c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos. 3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales: a) Los ficheros regulados por la legislación de régimen electoral. b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública. c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas. d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes. e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.		applies despite any provision, enacted after this subsection comes into force, of any other Act of Parliament, unless the other Act expressly declares that that provision operates despite the provision of this Part.

A la vista del análisis sobre el ámbito de aplicación de cada una de las normas referenciadas, podemos señalar que el ámbito de aplicación se divide en los siguientes aspectos:

- **objetivo o material:** dentro del ámbito objetivo de aplicación de las normas sobre protección de datos puede atenderse, a su vez, a los siguientes aspectos:

  - las normas que establecen disposiciones, como la Directiva 95/46/CE y la LOPD, que son aplicables tanto a los tratamientos automatizados como a los no automatizados (en soporte papel);
  - aquellas normas, como el Convenio 108 y la LOPD, que establecen disposiciones específicas para sistemas de datos personales de titularidad privada (sector privado) y de titularidad pública (Administraciones Públicas),
  - por último, todas las normas señalan excepciones en cuanto a su ámbito de aplicación, estableciendo que determinados tratamientos de datos de carácter personal quedan excluidos o pueden quedar fuera del régimen jurídico establecido por las mismas, así como otros tratamientos cuya regulación se remite a una norma especial o específica correspondiente, sin perjuicio de lo que establezca la que puede entenderse como norma "general" de protección de datos.

- **subjetivo:** en cuanto a que las disposiciones contenidas en las mismas establecen un ámbito de protección por el que quedan cubiertos las personas físicas y, en determinados supuestos, las personas jurídicas, como es el caso de la Ley de Argentina[13].

- **territorial:** siendo todas las normas de aplicación en el ámbito territorial correspondiente, si bien tal y como ocurre en el caso de la Directiva 95/46/CE y de la LOPD sus disposiciones pueden extenderse más allá de las fronteras en determinados supuestos expresamente previstos.

Conclusiones: al establecer el ámbito de aplicación de la norma sobre protección de datos, el legislador tiene que tener presentes diversos aspectos que determinarán qué tratamientos de datos personales van a quedar cubiertos o excluidos del régimen establecido por la misma. Así, dentro del ámbito de aplicación de la norma tiene que atenderse a cuál es su ámbito objetivo, subjetivo y territorial.

[13] Que así hemos visto señalaba en su artículo primero: *"Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal."*

Al analizar la LAI, y en cuanto a la aplicación de sus disposiciones, debe recordarse que sus disposiciones se dirigen exclusivamente a establecer obligaciones para determinados sujetos de la Administración Pública Federal (APF).

En definitiva, el legislador tendrá que establecer el ámbito de aplicación de la norma en virtud de los diferentes aspectos que vayan a tenerse en consideración y que determinarán los casos que quedarán sujetos a las disposiciones de la misma o excluidos. Así, por ejemplo, la norma sobre protección de datos podría regular la protección de datos personales de las personas físicas, excluyendo a las personas jurídicas, en los tratamientos de datos llevados a cabo tanto por Administraciones Públicas como por el sector privado. En consecuencia, la definición del ámbito de aplicación resulta esencial pues será sobre el que gire después el resto de la normativa.

1.3. Definiciones

Con el fin de poder comprender el verdadero significado de los términos empleados por las normas jurídicas, éstas con bastante frecuencia contienen las definiciones que en el contexto que regulan deben darse a cada uno de los conceptos implicados. De este modo, se recoge a continuación un análisis comparativo de las definiciones que recogen las normas que analizamos.

En el Convenio 108:

En primer lugar el Convenio 108 acoge las definiciones en su artículo 2 del siguiente modo:

- **Datos de carácter personal**: cualquier información relativa a una persona física identificada o identificable («persona concernida») (letra a).

- **Sistema de datos personales automatizado**: cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado (letra b).

- **Tratamiento automatizado**: se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión (letra c).

- **Autoridad controladora del sistema de datos personales:** la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del sistema de datos automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán (letra d).

En la Directiva 95/46/CE:

La Directiva 95/46/CE reúne también en su artículo 2 un conjunto de definiciones que ayudan a centrar la materia y a comprender el alcance de los términos incluidos en su texto normativo. A la vez que analizamos las suyas propias iremos haciendo referencia al contenido que las legislaciones nacionales que analizamos atribuyen a cada uno de los conceptos-

- **Datos personales:** Toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social (art. 2.a) de la Directiva 95/46/CE).

LOPD	LEY Nº 25326	PIPED Act
Datos personales		
Art. 3.a	**Art. 2**	**2**
Cualquier información concerniente a personas físicas identificadas o identificables.	Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.	"personal information"' means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

Tratamiento: Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción (art. 2.b) de la Directiva 95/46/CE).

LOPD	LEY Nº 25326.	PIPED Act
Tratamiento de datos		
Art. 3.c	**Art. 2.**	

Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.	Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.	

Fichero de datos personales: Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica (art. 2.c) de la Directiva 95/46/CE).

LOPD	LEY Nº 25326.	PIPED Act
Fichero de datos personales		
Art. 3.b)	**Art. 2.**	**2**
Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.	Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.	includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

Responsable del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario (art. 2.d) de la Directiva 95/46/CE).

LOPD	LEY Nº 25326.	PIPED Act
Responsable del tratamiento o del fichero		
Art. 3.d	**Art. 2**	**2**
Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.	Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.	includes an association, a partnership, a person and a trade union

Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate

datos personales por cuenta del responsable del tratamiento (art. 2.e) de la Directiva 95/46/CE).

LOPD	LEY Nº 25326.	PIPED Act
Encargado del tratamiento		
Art. 3.g		
Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.		

Tercero: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento (art. 2.f) de la Directiva 95/46/CE).

Destinatario: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios (art. 2.g) de la Directiva 95/46/CE).

Consentimiento del interesado: Toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan (art. 2.h) de la Directiva 95/46/CE).

LOPD	LEY Nº 25326.	PIPED Act
Consentimiento		
Art. 3.h		
Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.		

Además de estas definiciones de la Directiva europea, las normas que analizamos hacen referencia a otras definiciones que recogemos a continuación:

LOPD	LEY Nº 25326.	PIPED Act
Afectado o interesado. Titular de los datos		
Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo (art. 3.e). **Identificación del afectado:**	Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley. (art. 2 Ley nº 25326)	

cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada (art. 1.5 del R.D. 1332/94).		
Procedimiento de disociación		
Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable (art. 3.f).	Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable. (art. 2 Ley nº 25326)	
Cesión o comunicación de datos		
Toda revelación de datos realizada a una persona distinta del interesado (art. 3.i). **Cesión de datos:** toda obtención de datos resultante de la consulta de un fichero, la publicación de los datos contenidos en el fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada (art. 1.2 del R.D. 1332/94).		
Fuentes accesibles al público[14]		
Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los		

[14] El R.D 1332/94 definía datos accesibles al público como: *"los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo"*. Es necesario tener presente que esta definición tiene que interpretarse conforme a la LOPD, ya que el R.D. 1332/94 queda subsistente en tanto no se oponga a aquélla.

diarios y boletines oficiales y los medios de comunicación (art. 3.j).		
Datos especialmente protegidos/Dato sensibles		
Datos relativos a ideología, afiliación sindical, religión o creencia, origen racial, salud, vida sexual (art. 7.2 y 3 de la LOPD).	Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual (art. 2 Ley nº 25326)	
Bloqueo de datos		
La identificación y reserva de datos con el fin de impedir su tratamiento (art. 1.1 R.D. 1332/94).		
Transferencia de datos		
El transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional. (art. 1.6 R.D. 1332/94).		
Datos informatizados		
	Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado (art. 2 Ley nº 25326)	
Usuario de datos		
	Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos (art. 2 Ley nº 25326)	
Alternative format		
		with respect to personal information, means a format that allows a person with a sensory disability to read or listen to the personal information (Clause 2)

A efectos de la Transferencia Internacional de Datos, a cuyo régimen jurídico atenderemos en el apartado correspondiente del Informe, es necesario señalar aquí las siguientes definiciones que proporciona la **Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, por las que se rigen los movimientos internacionales de datos**:

- **Transferencia internacional de datos**: toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan

por objeto la realización de un tratamiento de datos por cuenta del responsable del sistema de datos personales (Norma primera).

- **Transmitente**: la persona física o jurídica, pública o privada, responsable del sistema de datos o tratamiento de los datos de carácter personal que son objeto de transferencia internacional (Norma primera).

- **Destinatario**: la persona física o jurídica, pública o privada, situada fuera del territorio español que recibe los datos transferidos (Norma primera).

Por su parte, la LAI aúna algunas definiciones en el artículo 3 relativas al tratamiento de datos personales llevado a cabo por la Administración Pública Federal en el desarrollo de las competencias que tienen atribuidas los sujetos obligados, y así establece, entre otras, las siguientes:

- **Datos personales**: la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten a su intimidad (fracción II del artículo 3 de la LAI).

- **Información**: la contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título (fracción V del artículo 3 de la LAI).

- **Información reservada**: aquella información que se encuentra temporalmente sujeta a alguna de las excepciones previstas en los Artículos 13 y 14 de la Ley (fracción VI del artículo 3 de la LAI).

- **Instituto**: el Instituto Federal de Acceso a la Información establecido en el artículo 33 de la Ley (fracción VII del artículo 3 de la LAI).

- **Sistema de datos personales**: el conjunto ordenado de datos personales que estén en posesión de un sujeto obligado (fracción XIII del artículo 3 de la LAI).

Conclusiones: si bien el establecimiento de definiciones en una norma puede restringir su interpretación, se plantea la posibilidad, tal y como se hace ya en la LAI, de incluir algunas definiciones que permitan conocer o concretar determinados aspectos de su aplicación en cuanto que sirvan de aclaración sobre los conceptos utilizados en la normativa.

Así, puede verse como a nivel internacional, las normas que regulan en diferentes ordenamientos jurídicos la protección de datos de carácter personal, y otras materias relacionadas con las nuevas tecnologías, establecen entre otras definiciones, las de: datos de carácter personal; interesado o afectado (titular de los datos); sistema de datos personales; responsable del sistema de datos o tratamiento; tratamiento de datos de carácter personal; encargado del tratamiento; cesión o comunicación de datos; consentimiento del interesado; bloqueo de los datos; etc.

2. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Con el fin de comprender mejor los principios aplicables en materia de protección de datos, debemos plantear, de una manera didáctica y doctrinal, que el tratamiento se puede estructurar en tres fases, cuya exposición resulta conveniente efectuar aquí para posteriormente poder conocer cómo se aplica la correspondiente normativa sobre protección de datos; interpretarlas y fijar las obligaciones del titular del sistema de datos personales (es decir, el responsable), teniendo en consideración los tres momentos o fases en que se desarrolla, o puede desarrollarse, el tratamiento de datos de carácter personal.

Estos tres momentos deben estar siempre presentes en el estudio de los principios de la protección de datos, los derechos de los ciudadanos y los procedimientos que les permitan ejercer sus derechos, y son:

- **Primera fase**: el momento de recabar los datos, bien sea directamente del interesado o de un tercero, en el que resulta transcedente su licitud y lealtad[15], con las características de conocimiento y, en su caso, consentimiento del interesado;

- **Segunda fase**: el momento del tratamiento de los datos, que pueden ser cruzados y relacionados en forma automática junto con otros datos, buscando definir un perfil determinado del afectado que incluso él mismo llega a desconocer, y

- **Tercera fase**: el momento de la utilización y, en su caso, comunicación a terceros de los resultados del tratamiento, conocida ésta última como "cesión o comunicación de datos", en la que, al igual que en la recogida y en el tratamiento, se tendrá que considerar el conocimiento y consentimiento del titular.

Los principios en los que comúnmente las leyes internacionales estructuran la protección de datos de carácter personal, los vamos a desarrollar en un orden que permita en la práctica seguir con aprovechamiento su utilización e implementación; es así que empezamos por el denominado principio del consentimiento por considerarle el eje central de la protección de datos.

[15] El concepto de lealtad que al figurar en una ley puede parecer, y lo es, un concepto jurídico indeterminado, tiene gran importancia por la referencia expresa y concreta que a él hace la ley española de protección de datos y, con mayor fuerza, la Directiva europea sobre el mismo tema.

2.1. Principio del consentimiento

La teoría general sobre la que gira el presente documento relativo a la protección de datos de carácter personal es el llamado "principio del consentimiento" que se puede resumir diciendo que el interesado es el único que decide cuándo, dónde y cómo se presentan sus datos al exterior, o se dan a conocer sus datos a terceros; esto es, el afectado tiene que otorgar su consentimiento para que se pueda realizar un tratamiento de sus datos de carácter personal desde la primera fase. Dicho de otra forma, en principio no se pueden tratar datos de carácter personal sin el consentimiento de su titular (del titular de los datos), salvo que la Ley indique lo contrario.

Sin perjuicio de lo anterior, es necesario tener en consideración que el consentimiento es un principio de la protección de datos exigido por la mayoría de los ordenamientos jurídicos europeos, si bien, no ocurre así en el ordenamiento inglés, en el que este principio no está presente específicamente del mismo modo, teniendo que llegarse de forma indirecta a él, mediante la aplicación del resto de principios en el sentido de que la protección de los interesados tendrá que garantizarse a través de su cumplimiento efectivo.

Este principio de consentimiento o la necesidad de que el tratamiento de datos de carácter personal se lleve a cabo con el consentimiento de los interesados puede estar sometido a las excepciones que la normativa establezca en su caso.

Los supuestos en los que se pueden tratar datos de carácter personal sin el consentimiento de los interesados podrían ser, entre otras, los relativos a obligaciones legales, es decir, porque se trate del ejercicio de las funciones de los poderes del Estado, o si el tratamiento deriva de una relación contractual de cualquier tipo, si los datos figuran en las denominadas fuentes de acceso al público, y, finalmente, cualesquiera otra que se prevea.

Asimismo, debe existir la posibilidad de que los interesados puedan revocar el consentimiento que hayan prestado. En este sentido, es beneficioso que la revocación no tenga atribuidos efectos retroactivos de forma que no afecte a los tratamientos de datos anteriores en los que sí se contaba con el consentimiento.

2.1.1. Forma del consentimiento

En otro orden de cosas, sería necesario prever con claridad cómo tiene que ser el consentimiento otorgado por los interesados para el tratamiento de sus datos de carácter personal, ya que ello podría suscitar problemas de prueba, y, además, teniendo en cuenta las diferentes categorías de datos. En definitiva, hay que especificar si se admite o no el consentimiento tácito y en qué casos, o, por el contrario, si siempre tiene que ser expreso o debe ser, incluso, expreso y por escrito, con las consecuencias que se deriven en cada situación.

El Convenio 108 no establece regulación alguna sobre la forma del consentimiento. Sin embargo, la Directiva 95/46/CE viene a establecer en su artículo 7 que:

> *"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:*
>
> *a) el interesado ha dado su consentimiento de forma inequívoca, o*
> *b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o*
> *c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o*
> *d) es necesario para proteger el interés vital del interesado, o*
> *e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o*
> *f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva."*

Por su parte, las normas nacionales correspondientes a los países que venimos analizando establecen que:

LOPD	LEY Nº 25326	PIPED Act
PRINCIPIOS RELATIVOS A LA LEGITIMACIÓN DEL TRATAMIENTO DE DATOS		
	Art. 5	**Schedule 1**
	Regla general	
El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa (art. 6.1).	1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.	4.3. The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

	El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.	
Sólo con consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical religión y creencias (art. 7.2).		4.3.1. Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).
Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente (art. 7.3).		4.3.2. The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.
Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado (art. 11.1).		4.3.3. An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.
		4.3.4[16]. The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any

[16] El apartado 4.3.4 del Anexo 1 continua con un ejemplo que dice: *"For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive."*

		information can be sensitive, depending on the context.
		4.3.5[17]. In obtaining consent, the reasonable expectations of the individual are also relevant.
		4.3.6. The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).
		4.3.7. Individuals can give consent in many ways. For example: (a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses; (b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties; (c) consent may be given orally when information is collected over the telephone; or; (d) consent may be given at the time that individuals use a product or service.

[17] El apartado 4.3.5. del Anexo continua igualmente con un ejemplo que dice: *"For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception."*

Excepciones		
Art. 6.2	**Art. 5**	**Art. 7.1**
		For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if (c) the collection is solely for journalistic, artistic or literary purposes; or
cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias;	b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;	
cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;	d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;	
cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o		(a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.	a) Los datos se obtengan de fuentes de acceso público irrestricto;	(d) the information is publicly available and is specified by the regulations. (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
	c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;	
	e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.	
Art. 11.2		**Art. 7.2**
a) Cuando la cesión está autorizada en una ley.		For the purpose of clause 4.3 of Schedule 1, and despite the note that

b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.		accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention; (b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual; (c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used; (c.1) it is publicly available and is specified by the regulations; or (d) it was collected under paragraph (1)(a) or (b).
Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos		

relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. (art. 7.2) Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. (art. 7.3) No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. (art. 7.6)		

		Art. 7.3
		For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization; (b) for the purpose of collecting a debt owed by the individual to the organization; (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records; (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province; (d) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization (i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or (ii) suspects that the information

		relates to national security, the defence of Canada or the conduct of international affairs; (e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure; (f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed; (g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation; (h) made after the earlier of (i) one hundred years after the record containing the information was created, and (ii) twenty years after the death of the individual whom the information is about; (h.1) of information that is publicly available and is specified by the regulations; (h.2) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or (i) required by law.
Revocación		
Art. 6.3	**Art. 5 Decreto**	**Schedule 1**
El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.	El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo. La revocación no tiene efectos retroactivos.	4.3.8. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.
El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable (art. 11.4)		

Además, y teniendo en cuenta uno de los objetivos de este informe, en el caso de la LOPD, el consentimiento del interesado legitima la realización de una TID

a un país tercero que no tenga un nivel equiparable de protección de datos, si bien nos remitimos al apartado de este Informe en el que se analiza esta cuestión.

Según se puede observar en la tabla comparativa anterior, las tres normas establecen como regla general la necesidad de contar con el consentimiento para el tratamiento de datos de carácter personal, ya sea un consentimiento inequívoco[18], como en el caso de la norma española, libre, expreso e informado en Argentina o, como en el caso de la norma canadiense, que se requiere "conocimiento y consentimiento". En México, aunque no se refiere al tratamiento de los datos sino a su difusión, distribución y comercialización, el consentimiento es expreso, por escrito **o** por un medio de autenticación similar, tal y como exige el artículo 21 de la LAI.

En la legislación canadiense se regulan otros aspectos relativos al consentimiento que de manera más detallada, como la forma del consentimiento que variará en función de las circunstancias y del tipo o categorías de datos de los que se trate; incluso se prevé que el consentimiento puede otorgarse de diferentes formas, contemplando varios ejemplos sobre cómo proporcionarlo. En España también, para los datos especialmente protegidos se exige consentimiento expreso y, en su caso, por escrito, y ello con el fin de ofrecer un mayor grado de protección.

Tal y como se ha visto, en Argentina el consentimiento tiene que ser libre, expreso e informado y sobre esta última característica el artículo 5 del Decreto define qué ha de entenderse por consentimiento informado, estableciendo:

> *"El consentimiento informado es el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el art. 6 de la Ley nº 25326."*

El principio de consentimiento en México se encuentra regulado en los artículos 21 y 22 de la LAI pero sólo en relación con la cesión o comunicación de datos a terceros. no dice cómo se tienen los datos, así que lo que hay que decir es que hay que prever la licitud del tratamiento, en concreto mediante la obtención del consentimiento, en su caso y en los Lineamientos vigésimo segundo y vigésimo tercero. Mientras que para las tres normas anteriores se requiere el consentimiento de los interesados para el tratamiento de sus datos

[18] Lo que, conforme a la definición dada en la letra h) del artículo 3, significa: *"toda **manifestación de voluntad, libre, inequívoca, e informada**, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".*

de carácter personal, en México no se dice nada acerca de la necesidad del consentimiento para el tratamiento de datos de carácter personal pero sí que se requiere del consentimiento, aunque para una fase posterior, en los términos que establece el artículo 21 de la LAI, que prevé:

> *"Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones,* ***salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información****."*

En este mismo sentido se expresa el Lineamiento vigésimo segundo al establecer que:

> *"Las dependencias y entidades no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones,* ***salvo que se cuente con el consentimiento expreso de los individuos*** *a que haga referencia la información."*

Tal y como hemos especificado en el apartado de Definiciones, en México el término "tratamiento" no sólo se refiere a los actos regulados en el artículo 21 de la LAI de "*difundir, distribuir o comercializar*" los datos personales, sino que se incluye dentro de este concepto la recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación y transmisión de datos personales. Por ello, sería recomendable establecer la necesidad del consentimiento para el tratamiento, en sentido amplio, de los datos personales, dado que como hemos visto, el consentimiento es uno de los principios que legitima el tratamiento de datos de carácter personal de los interesados.

Sobre este principio de consentimiento todas las normas objeto de análisis establecen excepciones a su necesidad para tratar datos de carácter personal. En concreto, las normas española, argentina y canadiense recogen la excepción al requerimiento del consentimiento cuando se trate de datos recogidos u obtenidos de fuentes disponibles para el público.

Otras excepciones coincidentes en las normas española y argentina es sobre aquellos datos que hayan sido recabados para el ejercicio de las funciones propias de los poderes del Estado y cuando los datos deriven de una relación contractual y sean necesarios para su desarrollo o cumplimiento.

En cuanto a las normas española y canadiense hay que destacar que permiten como excepción al consentimiento cuando el tratamiento es en interés del titular de los datos, aunque en España se puntualiza que este interés ha de ser "vital" del interesado.

Tanto la legislación argentina como la candiense prevén ciertas excepciones al consentimiento que no se encuentran en el resto de las legislaciones. En concreto, la norma argentina, por un lado, prevé un listado de datos para cuyo tratamiento no será necesario el consentimiento y, por otro, si se trata de operaciones financieras. En relación con la Ley de Protección de Datos de Canadá, entre el listado de excepciones que se establecen encontramos que una de ellas, relativa a estudios estadísticos e investigaciones, prevista en el artículo 7.2 letra (c), es similar a la excepción prevista en la fracción II del artículo 22 de la LAI, que regula las excepciones al consentimiento y, en concreto, prevé:

> *"No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:*
>
> *I. (Se deroga)[19].*
> *II. **Los necesarios por razones estadísticas, científicas o de interés general** previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;*
> *III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;*
> *IV. Cuando exista una orden judicial;*
> *V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y*
> *VI. En los demás casos que establezcan las leyes."*

En cuanto a la posibilidad de revocar el consentimiento prestado, hay que señalar que tanto las normas analizadas, a través de la tabla, como los Lineamientos regulan la revocación del consentimiento. En concreto, el Lineamiento 23 viene a establecer lo siguiente:

> *"Los titulares de los datos podrán otorgar y revocar su autorización para que se difundan, distribuyan o comercialicen sus datos personales a terceros.*

[19] La fracción I del artículo 22 de la LAI decía: *"Los necesarios para la prevención o el diagnóstico médico, la prestación de asistencia médica o la gestión de servicios de salud y no pueda recabarse su autorización"*.

La autorización deberá ser por escrito con firma autógrafa y anexando copia de identificación oficial del titular de los datos".

Aunque, todas las normas establecen la revocabilidad del consentimiento prestado hay que señalar que en los Lineamientos la revocación se refiere a la difusión, distribución o comercialización ya que así estaba previsto en la regla general del principio de consentimiento, y no en el tratamiento. Sin embargo, tal y como se indicó al examinar la regla general del consentimiento en las legislaciones que se analizan, hay que atender a la recomendación que se hacía sobre la necesidad de prever el consentimiento para el tratamiento, en sentido amplio, de los datos personales.

Asimismo, hay que destacar una peculiaridad de la revocación del consentimiento en las normas española y argentina, puesto que atribuyen a la revocación efectos irretroactivos, de manera que no pueda afectar a los tratamientos de datos anteriores en los que sí se contaba con el consentimiento.

Conclusiones: al establecer una regulación sobre protección de datos debe partirse de los principios de la protección de datos, entre los que destaca el del consentimiento. En este sentido, es necesario tener en consideración que el principio del consentimiento da lugar, a su vez, a la necesidad de analizar varios aspectos, comenzando por el propio significado del consentimiento que es uno de los principios que legitiman el tratamiento de datos de carácter personal. Así, en la mayoría de las normas analizadas el consentimiento es uno de los principios que legítima el tratamiento de datos personales. Además, este consentimiento, según el análisis de estas normas, se configura como una manifestación de voluntad, libre, específica, informada, y como se señala en el caso de la LOPD, inequívoca, mediante la que el interesado consienta el tratamiento de sus datos de carácter personal.

Establecida la definición del consentimiento o, mejor dicho, una vez atendido al concepto que del consentimiento proporcionan las normas que venimos analizando, el siguiente aspecto a tener en consideración es la forma en que ha de otorgarse el consentimiento, estando aceptada en la legislación internacional sobre protección de datos la posibilidad de que, como norma general, no se establezca un requisito concreto al respecto, de manera que se admite tanto el consentimiento expreso como el tácito, si bien en este segundo caso se plantea la necesidad de probar que el consentimiento ha sido obtenido por el responsable del tratamiento.

No obstante, la aceptación del consentimiento tanto expreso como tácito resulta independiente del requisito de forma, que en varias de las normas analizadas, se exige para el tratamiento de datos especialmente protegidos, tales como los relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. Dada la necesidad de establecer un mayor grado de protección, en estos supuestos las normas exigen que el consentimiento del interesado, cuando sea necesario, se otorgue en una determinada forma, siendo éste expreso y, en su caso, por escrito.

Por último, todas las normas analizadas exigen que se obtenga, como norma general, el consentimiento de los interesados para el tratamiento de sus datos personales, si bien también contemplan determinadas excepciones en casos previstos expresamente por la Ley en los que dicho consentimiento no es necesario. En cuanto a la obtención del consentimiento, es necesario distinguir el consentimiento para la recogida y tratamiento de datos de carácter personal y el consentimiento para la cesión o comunicación de datos (o términos similares como distribución, utilizado por la LAI), debiendo remitirnos a pesar de lo indicado aquí, al apartado relativo al análisis del principio de consentimiento del tratamiento.

En definitiva, la inclusión del principio del consentimiento en una Ley de Protección de Datos requiere tener en consideración los diferentes aspectos que hemos señalado, siendo necesario que se parta de su propia definición y posteriormente concretar la forma en que éste habrá de ser otorgado para el tratamiento los datos personales.

2.2. Principio de calidad de los datos

Independientemente de lo que ya hemos expresado sobre la necesidad del consentimiento para recabar y tratar datos de carácter personal, en su caso comunicándolos a terceros, y las excepciones al mismo, los datos que se recaben deben ser pertinentes, adecuados y no excesivos para el fin que se pretenda en su tratamiento, además de que no podrán permanecer en el sistema de datos personales por tiempo mayor al necesario para cumplir con la finalidad para la que se obtuvieron.

La calidad de los datos, fuente de múltiples conflictos interpretativos en las normas sobre protección de datos que analizamos, se puede resumir indicando que la información, o los datos que se recaban o que se registran en un sistema de datos personales, debe ser exacta, mantenida al día, apropiada para el fin

para el que fue almacenada y obtenida por medios legales y, añadimos nosotros, leales.

Ello exige, girando sobre el concepto de pertinencia de los datos, de acuerdo con el ámbito y la finalidad para los que se hayan obtenido, que vaya acompañado de su exactitud y su actualización.

La utilización de los datos personales de acuerdo con el fin para el que fueron obtenidos -adecuación al fin-, junto con la cancelación y sustitución de oficio en determinados supuestos -debido a su inexactitud total o parcial- y el almacenamiento de forma que el titular pueda ejercer su derecho de acceso, son los complementos que garantizan la calidad exigida por la norma.

De esta forma, cuando los datos registrados sean inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, existiendo también la obligación de cancelarlos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

A continuación, vamos a atender a las previsiones que, sobre el principio de calidad de los datos, se contiene en las diferentes normas que venimos analizando.

En el Convenio 108:

En cuanto a la calidad de los datos, el Convenio 108 dispone en su artículo 5 que:

> *"Los datos de carácter personal que sean objeto de un tratamiento automatizado:*
>
> *a) Se obtendrán y tratarán leal y legítimamente;*
> *b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;*
> *c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;*
> *d) serán exactos y si fuera necesario puestos al día;*
> *e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado."*

En la Directiva 95/46/CE:

La Directiva 95/46/CE establece en su artículo 6 que:

"1. Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;
b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;
c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;
e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1."

En las normas nacionales:

LOPD	LEY Nº 25326	PIPED Act
PRINCIPIOS RELATIVOS A LA CALIDAD DE LOS DATOS		
Art. 4	**Art. 4**	**Schedule 1**
1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.	1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.	4.4. The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means. 4.6. Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. 5.3. An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará	3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.	4.4.1. Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the

incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.		purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8). 4.6.2. An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.	4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.	4.4.2. The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.	5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.	4.4.3. This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de	7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.	4.5. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

determinados datos.		
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.	6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.	4.5.1. Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1). 4.5.2. Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods. 4.5.3. Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.	2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.	
		4.5.4. This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).
		4.6.1. The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.
		4.6.3. Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-

		date, unless limits to the requirement for accuracy are clearly set out.

En términos generales, existe una regulación similar en las legislaciones de España, Argentina, Canadá y México en relación con el principio de calidad de los datos. Con el objeto de señalar estas similitudes, a continuación se incluye lo dispuesto en el artículo 20 de la LAI:

> *"Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:*
>
> *II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;*
> *[...]*
> *IV. Procurar que los datos personales sean exactos y actualizados;*
> *V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, ..."*

Asimismo, distintos Lineamientos desarrollan esta cuestión, en concreto, los siguientes:

> *"**Decimocuarto.** Sólo se podrá tratar datos personales cuando estos sean adecuados, pertinentes y no excesivos en relación con las finalidades específicas y legítimas para las que se hayan recolectado.*
>
> *...*
>
> ***Decimoséptimo.** El tratamiento de datos de carácter personal no podrá realizarse para fines incongruentes con aquellos para las que los datos hubieran sido recolectados, con excepción de aquellos que se utilicen con finalidades históricas, estadísticas o científicas.*
>
> *...*
>
> ***Decimoctavo.** Se deberán evitar tratamientos de datos personales que representen un riesgo para los derechos y libertades de los titulares.*
>
> *...*
>
> ***Vigésimo.** Los datos de carácter personal no se conservarán en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados, con excepción de aquellos datos tratados por cuestiones históricos, estadísticos o científicos."*

Un aspecto a destacar en relación con este principio de calidad de los datos y previsto en las normas española, argentina y mexicana es el relativo a la

prohibición de recabar datos por medios desleales, fraudulentos o ilícitos. En este sentido, el Lineamiento decimoquinto dispone:

> *"Se prohíbe la recogida de datos por medios fraudulentos o ilícitos."*

Asimismo, hay que tener en cuenta el artículo 4 del Decreto argentino que prevé lo siguiente:

> *"Para determinar la lealtad y buena fe en la obtención de los datos personales, así como el destino que a ellos se asigne, se deberá analizar el procedimiento efectuado para la recolección y, en particular, la información que se haya proporcionado al titular de los datos de acuerdo con el artículo 6° de la Ley N° 25.326.*
>
> *Cuando la obtención o recolección de los datos personales fuese lograda por interconexión o tratamiento de archivos, registros, bases o bancos de datos, se deberá analizar la fuente de información y el destino previsto por el responsable o usuario para los datos personales obtenidos.*
>
> *El dato que hubiera perdido vigencia respecto de los fines para los que se hubiese obtenido o recolectado debe ser suprimido por el responsable o usuario sin necesidad de que lo requiera el titular de los datos."*

Previsión que, por otra parte, también se encuentra en el Convenio 108 y en la Directiva 95/46/CE al exigir el que tratamiento de datos se haga de forma legal y leal, como ya hemos señalado anteriormente.

Conclusiones: el principio de calidad de los datos supone, en las normas que analizamos e incluida la LAI, que los datos personales de los interesados sólo puedan tratarse cuando sean adecuados, pertinentes y no excesivos en relación con la finalidad o los propósitos para la que los datos hayan sido obtenidos. Este principio de calidad de los datos es fuente de numerosas interpretaciones en todas las normas analizadas, en el sentido de que la calidad de los datos tiene que analizarse en cada tratamiento de datos de carácter personal.

Además de lo anterior, el principio de calidad de los datos supone, tal y como hemos visto en todas y cada una de las normas estudiadas, que éstos no puedan recabarse por medios que resulten fraudulentos, debiendo garantizarse a los interesados que el tratamiento de sus datos de carácter personal sea legal y, como hemos señalado anteriormente, también leal.

2.3. Principio de información en la recogida de datos

Es un principio general de protección de datos que todo ciudadano tiene derecho a ser informado de determinados extremos cuando se le solicitan datos de carácter personal con el fin de que conozca quién, cómo y para qué los va a tratar, así como poder ejercitar, en su caso, los derechos que la Ley le reconoce.

En general, como veremos a continuación, las diferentes normas disponen que cuando se recaben datos de una persona para ser utilizados mediante un tratamiento, automatizado o no, , o mantenerlos en un soporte susceptible de tratamiento automatizado, se debe realizar de una forma legal y leal; ello incluye que el afectado sea informado -de modo expreso, preciso e inequívoco-, no sólo de la finalidad de la recogida sino también de los destinatarios de la información, advirtiéndole si tiene o no obligación de contestar a las preguntas que se le realizan y de cuáles pueden ser las consecuencias en el caso de que se niegue a contestar o a proporcionar los datos.

Habrá que informarle también del derecho que tiene a acceder para saber los datos que de él se mantienen por el responsable del sistema de datos y, en su caso, exigir la rectificación o cancelación de los mismos cuando sean inexactos, obsoletos o no adecuados al fin perseguido. También deberá ser informado de su derecho de oposición al tratamiento de datos de carácter personal. Como es natural, para que pueda ejercer sus derechos, se deberá notificar también al afectado sobre la identidad y dirección del responsable del sistema de datos o, en su caso, de su representante, si esta figura estuviera prevista en la normativa sobre protección de datos para aquellos casos en los que el responsable actúe en el territorio de aplicación de la norma mediante dicho representante.

Por otro lado, hay que tener en cuenta que, asimismo, puede haber ocasiones en las que los datos personales puedan ser recabados de determinadas fuentes que dada su finalidad pueden ser accesibles a cualquiera sin necesidad de contar con el consentimiento de los interesados (por ejemplo, los listados telefónicos), es decir, de las conocidas como fuentes accesibles al público que se prevén en algunas de las normas referidas anteriormente. Si se recogieran datos de carácter personal de una fuente de estas características, los interesados no pueden ver mermado completamente su derecho a controlar quién, cómo, dónde y para qué trata sus datos. De forma que, puede preverse que en determinadas circunstancias, quien use los datos de carácter personal para ponerse en contacto con su titular para, por ejemplo remitirle comunicaciones publicitarias, sería conveniente que le informara de quién es,

de dónde recogió los datos, para qué los quiere y cuáles son los derechos que le asisten como titular de los datos.

Aunado a lo anterior, y en estrecha relación tal y como vamos a ver al analizar las normas internacionales sobre protección de datos, puede diferenciarse aquellos supuestos en los que se informe al interesado cuando los datos sean recabados directamente de él de aquellos otros en los que los datos se recaben a través de un tercero.

Asimismo, hay que tener en cuenta otras formas de obtener los datos de carácter personal como a través de formularios o a través de Internet debiendo, de la misma forma, cumplir con el principio de información en todo caso.

<u>En el Convenio 108:</u>

El artículo 8 del Convenio 108 establece:

> *"Cualquier persona deberá poder:*
>
> *a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero."*

<u>En la Directiva 95/46/CE:</u>

La Directiva 95/46/CE dedica dos preceptos de su articulado a regular el principio de la información desde dos vertientes, por un lado, la información que hay que proporcionar en el caso de que los datos se obtengan del propio interesado, en su artículo 10, y por otro lado, la información a proporcionar cuando los datos no se hayan recabado del propio interesado, en su artículo 11.

En concreto, el artículo 10, sobre la información en caso de obtención de datos recabados del propio interesado establece:

> *"Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:*
>
> *a) la identidad del responsable del tratamiento y, en su caso, de su representante;*
> *b) los fines del tratamiento de que van a ser objeto los datos;*

c) cualquier otra información tal como:
- *los destinatarios o las categorías de destinatarios de los datos,*
- *el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,*
- *la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado."*

Por su parte, el artículo 11, sobre la información cuando los datos no han sido recabados del propio interesado, contempla:

"1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;
b) los fines del tratamiento de que van a ser objeto los datos;
c) cualquier otra información tal como:
- *las categorías de los datos de que se trate,*
- *los destinatarios o las categorías de destinatarios de los datos,*
- *la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.*

2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas."

A continuación se analiza este principio de información en las normas sobre protección de datos de España, Argentina y Canadá.

LOPD	LEY Nº 25326	PIPED Act
DERECHO DE INFORMACIÓN DEL INTERESADO		
Art. 5	**Art. 6**	**Schedule 1**
1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior. 3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.	Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.	4.2. The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa,		4.2.1. The organization shall document the purposes for which personal information is collected in order to comply with the

precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.		Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).
5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.		4.2.2. Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.
		4.2.3. The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.
		4.2.4. When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an

		elaboration on consent, please refer to the Consent principle (Clause 4.3).
		4.2.5. Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.
		4.2.6. This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).
		Art. 6
		The designation of an individual under clause 4.1 of Schedule 1 does not relieve the organization of the obligation to comply with the obligations set out in that Schedule.
Art. 27		
1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario. 2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.		
Art. 11.3		
Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.		

En España, el principio de información se regula desde dos puntos de vista. Por un lado, el artículo 5 regula la información que se ha de proporcionar a los interesados a los que se les recaben sus datos (art. 5, apartados 1 a 3) y, por otro, la información que se proporcionará a los propios titulares de los datos cuando los datos hayan sido recabados de terceros (art. 5.4 y 5.5).

En México el principio de información se ciñe a informar al interesado del propósito del tratamiento de sus datos, si bien se requiere que dicha

información conste en un documento que se ponga a disposición de los individuos, y queda regulado en el artículo 20 de la LAI que prevé:

> *"Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:*
>
> *[...]*
>
> *III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;"*

En este mismo sentido se expresa el Lineamiento, incluso yendo más allá al hablar de entregar un documento, ya no sólo poner a disposición del titular, en su apartado decimosexto, al contemplar que:

> *"A partir del momento en el cual se recaben datos personales, la dependencia o entidad deberá entregar al titular de los datos un documento en el que se establezcan los propósitos de la recogida."*

No obstante, por otro lado, en relación con este principio de información a los interesados y teniendo en cuenta lo regulado en la legislación mexicana, hay que destacar que el resto de las normas que se han analizado a través de la tabla anterior reflejan como información obligatoria para el interesado, no sólo los propósitos y las finalidades a las que se van a dedicar los tratamientos de los datos sino otros muchos aspectos como la existencia de un sistema de datos, los destinatarios de los datos, la identidad y domicilio del responsable, el carácter obligatorio o facultativo de la respuesta a las preguntas planteadas, las consecuencias de proporcionar los datos y la negativa de hacerlo, la posibilidad del ejercicio de los derechos de acceso, rectificación, cancelación o supresión y oposición.

En la legislación española se prevé la posibilidad de que los datos sean recabados por una persona distinta del propio interesado (artículo 5.4 de la LOPD) e incluso se establecen excepciones tasadas a este deber de información, como cuando así lo prevea una ley; el tratamiento tenga fines históricos, estadísticos o científicos, si informar al interesado requiere un esfuerzo desproporcionado a criterio del órgano de control y atendiendo a determinadas circunstancias y si los datos proceden de fuentes accesibles al público.

Por lo tanto, y en atención a las previsiones contenidas en las normas analizadas sería conveniente que la legislación mexicana ampliar el deber de

información a los interesados a los que se les soliciten sus datos en caso de llevar a cabo una regulación sobre protección de datos, ya que es importante conocer la finalidad o los propósitos del tratamiento pero también tienen la misma importancia, entre otros aspectos, conocer quién es el responsable del tratamiento y dónde puede el interesado ejercer sus derechos, sin perjuicio de que exista un registro público de sistemas de datos de carácter personal. En definitiva, se trata de garantizar al interesado que sus datos van a ser tratados de forma legal y leal, a lo que sólo puede llegarse mediante el cumplimiento de los principios de la protección de datos, entre los que se encuentra éste de información al interesado. Sin embargo, en este mismo sentido, la obligación de poner a disposición del individuo el documento que contenga esta información, si bien es una garantía mayor de cara al individuo, podría originar problemas logísticos, porque no siempre esa información consta en un documento, aunque sí se dé al individuo.

Por último, es necesario destacar que a diferencia del resto de las normas, la norma española establece la obligación de informar al interesado de la primera cesión que se realice de sus datos, con indicación de la finalidad del sistema de datos, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario. No obstante, esta referencia debe entenderse hecha aquí sin perjuicio de lo que, en su caso, pudiera indicarse al analizar el principio de cesión o comunicación de datos.

Conclusiones: el principio de la información en la recogida de datos de carácter personal determina que el interesado tenga que ser informado, tanto cuando los datos son recabados directamente de él como cuando se recogen a través de un tercero, de determinados extremos que le van a permitir conocer para qué se le piden sus datos, cómo van a ser utilizados, por quién y qué derechos tiene en relación con el tratamiento de estos datos.

Es decir, el principio de información supone que el interesado esté en disposición de poder controlar el tratamiento de sus datos de carácter personal ya que sólo a través del ejercicio de sus derechos podrá instar al responsable del tratamiento a, por ejemplo, cancelar o modificar sus datos personales. Este ejercicio de los derechos sólo será posible, a su vez, si el interesado conoce en todo momento a quién tiene que dirigirse.

Además, este principio de información, sin perjuicio de las excepciones que puedan preverse en la norma para determinados supuestos en los que no sea necesario informar al interesado, tiene que garantizarse con independencia de

cuál sea el medio, electrónico o no, utilizado para la recogida de datos de carácter personal.

2.4. Principio de categorías especiales de datos o datos especialmente protegidos

Como su nombre indica, los datos especialmente protegidos hacen referencia a una categoría especial de datos que, por su especial naturaleza, requieren de un mayor grado o nivel de protección en aras a garantizar la privacidad de los ciudadanos. Todas las normas internacionales sobre protección de datos hacen referencia, de una u otra manera, a estos datos especialmente protegidos, refiriéndose a ellos en esta forma o denominándolos categorías especiales o particulares de datos. Hemos optado por utilizar esta denominación porque es neutra, es decir, no se refiere a ninguna apreciación subjetiva, mientras que otras nomenclaturas utilizadas, como la de datos sensibles (que, por cierto, es la que utiliza la ley argentina), entendemos se aleja de esa neutralidad y añade percepciones que preferimos evitar, escogiendo el término utilizado por la norma comunitaria.

La especial protección a la que se hace referencia, se concreta en la práctica legal, en muchas ocasiones, como ya hemos expuesto anteriormente, en la necesidad de que se obtenga, cuando sea necesario, el consentimiento del interesado o afectado en una determinada forma, pudiendo ser este expreso y, en su caso, por escrito. Además, las normas que analizamos establecen otras previsiones en relación con el tratamiento de estos datos de carácter personal.

En el Convenio 108:

El artículo 6, bajo el título *categorías particulares de datos*, establece que

> *"Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales".*

En la Directiva 95/46/CE:

En su artículo 8 regula el *tratamiento de categorías especiales de datos*, de la siguiente manera:

"1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad".

En las normas nacionales:

LOPD	LEY Nº 25326.	PIPED Act
Datos especialmente protegidos		
Art. 7	**Art. 7**	**Clause 4.3.4. of the Schedule 1**
De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.	1. Ninguna persona puede ser obligada a proporcionar datos sensibles.	The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context.
2.Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3.Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. 6. No obstante lo dispuesto en los	Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.	

apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.		
Son datos especialmente protegidos: 1-los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. 2- Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual.	Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.	
Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.	Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles.	
Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.	Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.	
Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas	Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones	

competentes en los supuestos previstos en las respectivas normas reguladoras.	respectivas."	

En primer lugar, todas las normas analizadas contienen previsiones sobre datos especialmente protegidos, lo que determina que se trata de datos de una naturaleza especial que por su íntima conexión con la persona, y, en su caso, la mayor peligrosidad de su tratamiento ilícito, requieren de mayor protección.

En segundo lugar, y en respuesta a esta necesidad de un mayor grado de protección, como particularidades al derecho de consentimiento, la LOPD establece una categoría especial de datos de carácter personal a los que denomina datos especialmente protegidos, requiriendo que su tratamiento se lleve a cabo, salvo que la Ley disponga otra cosa, con el consentimiento expreso y, en su caso, por escrito del interesado. Estos datos que deben ser objeto de especial protección[20]; se rigen por las reglas especiales que se establecen el artículo 7 de la LOPD.

Siendo el consentimiento del afectado, como ya hemos indicado, necesario para recabar y tratar datos de carácter personal, *"salvo que la ley disponga otra cosa"*; y pudiendo ser este consentimiento tácito[21]; sin embargo, cuando se trata de los datos que el artículo 7 de la LOPD considera especialmente protegidos y a los que hacemos referencia, el consentimiento debe ser expreso, indicando, como mayor garantía, que en el caso de los datos a que se refiere el artículo 16.2. de la Constitución Española[22] y los datos referentes a la afiliación sindical, el consentimiento debe, además de ser expreso, otorgarse por escrito.

Se completa la garantía sobre los datos que se refieran a la ideología, religión y creencias, y la exigencia de protección especial, al indicar el artículo 7 de la LOPD que, además,

> *"Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo"*,

al tiempo que se prohíbe la creación de sistemas de datos personales con la finalidad exclusiva de almacenar datos de carácter personal que revelen la

[20] En términos generales diremos que se trata de los datos referentes al origen racial, a la salud y a la vida sexual por un lado y, por otro lado, a la ideología, afiliación sindical, religión y creencias.
[21] Es necesario insistir en que, aun siendo válido el consentimiento tácito, acudiremos a él solamente en los casos en que sea absolutamente necesario, debido a las dificultades de prueba que tiene.
[22] Que son los que se refieren a la ideología, religión y creencias.

ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Esta protección reforzada se concreta también en la cesión o comunicación de datos a terceros, siendo necesario que el consentimiento del interesado reúna los requisitos indicados anteriormente, salvo que concurra alguna excepción legal.

A diferencia de las leyes española y argentina, la ley canadiense no entra a detallar qué datos se consideran sensibles o especialmente protegidos y por tanto no adopta respecto de ellos ninguna medida especial de tratamiento como ocurre en las otras legislaciones referidas.

La normativa mexicana que analizamos tampoco hace distinción alguna en lo que a datos de carácter personal se refiere. En este sentido, nuestra experiencia y nuestra recomendación de cara a elaborar una normativa específica que regule la protección de datos personales es la de considerar que hay datos que por la información que contienen de su titular deben ser considerados con especial cautela dado que pueden comprometer al titular en algún sentido o, mejor dicho, que afectan o pueden afectar a su intimidad de una manera especial[23].

Conclusiones: el análisis de las normas internacionales de protección de datos proporciona criterios suficientes para recomendar que en el desarrollo de una norma que regule la protección de datos de carácter personal se contemple las diferentes categorías de datos de carácter personal que puedan establecerse incluyendo al mismo tiempo las previsiones oportunas y necesarias para garantizar su protección mediante, por ejemplo, el reforzamiento del principio de consentimiento al exigir una determinada forma.

Los datos especialmente protegidos constituyen una cuestión fundamental en el establecimiento de una regulación sobre protección de datos, ya que se refieren o pueden referirse a cuestiones íntimas de los interesados, que son los

[23] En este sentido, debería tenerse en consideración el establecimiento de una clasificación de datos personales, agrupándolos en torno al criterio de la mayor o menor confidencialidad. *"La confidencialidad de un dato puede ser estudiada desde una perspectiva general o desde el ámbito o dominio del dato sobre el entorno. No todos los datos están sujetos al mismo grado de confidencialidad, ni tan siquiera, los mismos datos están sujetos siempre al mismo grado de confidencialidad, dependiendo de circunstancias particulares del entorno en el que se está trabajando o actuando. Entendemos por confidencialidad el mayor o menor secreto con el que se van a guardar o tratar datos personales."Profesor Dr. Miguel Ángel Davara Rodríguez. Manual de Derecho Informático. 6ª Edición. Aranzadi. Pamplona 2004*

titulares de los datos, y que determinan la explicación de un régimen jurídico reforzado para su protección.

2.5. Principio de seguridad

La seguridad[24] en materia de protección de datos, debe ser extremada al máximo para impedir el acceso a los sistemas de datos personales, en particular, y a los datos en general, a personas no autorizadas o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos; pero la seguridad debe ser también tenida en cuenta para garantizar el tratamiento de datos dentro de los límites permitidos por la norma y con respeto a los derechos del afectado.

Las medidas de seguridad tienen por objeto garantizar la confidencialidad y la integridad de los datos personales evitando su alteración, pérdida, transmisión y acceso no autorizado. En definitiva, lo que se pretende es preservar la confidencialidad e integridad de la información que es objeto de tratamiento en los sistemas de información que contienen datos personales, debiendo adoptarse para ello las medidas de índole técnica y organizativa por quienes, por cualquier título ya sea un responsable del sistema de datos personales o un encargado del tratamiento, posean o traten de datos personales.

En el Convenio 108:

De esta forma el Convenio 108 recoge en su artículo 7 la necesidad de adoptar medidas de seguridad disponiendo que:

> *"Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados."*

En la Directiva 95/46/CE:

La Directiva 95/46/CE, señala en su artículo 17 la obligación del responsable del tratamiento de adoptar medidas de seguridad en los siguientes términos:

[24] Seguridad que puede ser entendida en tres aspectos, física, lógica y jurídica que deben ocupar un lugar prioritario en la implantación de los nuevos servicios y en todo tratamiento automatizado y/o telemático de datos de carácter personal, siendo importante el papel que debe jugar la seguridad y, consecuentemente, la auditoria de la seguridad.

"Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente."

La primera conclusión que podemos sacar de estos preceptos es la de una clara obligación de adoptar las medidas de seguridad necesarias para proteger los datos contenidos en los sistemas de datos de carácter personal. De este modo, se hace referencia a medidas "apropiadas", medidas "técnicas y organizativas adecuadas", matizando la Directiva europea en este punto la necesidad de que las medidas no sólo sean de carácter técnico sino que también deben ser de carácter organizativo, en relación con las personas implicadas en el tratamiento de datos.

El riesgo que representa el tratamiento y la naturaleza de los datos son los criterios establecidos por la Directiva para determinar las medidas de seguridad que se tienen a aplicar para garantizar la integridad y confidencialidad de la información.

El apartado segundo del artículo 17 de la Directiva que analizamos, establece la necesidad de que además del responsable del sistema de datos personales, deba observar las medidas de seguridad exigidas el encargado del tratamiento que proceda a realizar un tratamiento de los datos por cuenta del responsable del sistema de datos personales. Es decir, las medidas de seguridad son, además de un principio, una obligación de quien trata datos de carácter personal por cualquier título, ya sea como responsable o como encargado, debiendo hacerlas cumplir a su vez, por las personas que se encuentren a su

cargo y accedan a datos de carácter personal para el cumplimiento de sus funciones.

Por último, se hace referencia a que las medidas de seguridad que se decida adoptar deberán reflejarse en un documento escrito o en otro medio que permita acreditar su adopción y cumplimiento.

En las normas nacionales:

Las normas que comparativamente venimos analizando hacen referencia a esta obligación de adoptar las medidas de seguridad en los términos que reflejamos en la tabla que incluimos a continuación:

LOPD	LEY Nº 25326.	PIPED Act
Seguridad de datos		
Art. 9[25]	**Art. 9**	**Clause 4.7. of the SHEDULE 1.**
1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.	1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.	Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4. The methods of protection should include (*a*) physical measures, for

[25] Es necesario tener presente que este artículo ha sido desarrollado por el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (en adelante, Reglamento de Medidas de Seguridad o, también, R.D. 994/1999) que se encuentra subsistente en virtud de la Disposición transitoria tercera de la LOPD.

		example, locked filing cabinets and restricted access to offices; (*b*) organizational measures, for example, security clearances and limiting access on a ``need-to-know'' basis; and (*c*) technological measures, for example, the use of passwords and encryption. Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information. Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

Del análisis de esta normativa destacan los siguientes criterios que podríamos denominar básicos para lo que a la adopción de las medidas de seguridad se refiere y son entre otros:

1.- Las **personas obligadas a adoptar las medidas de seguridad** son además del responsable del sistema de datos, como hemos visto en al Directiva y en la LOPD, los encargados del tratamiento, o el usuario al que se refiere la Ley argentina.

2.- El **carácter de las medidas de seguridad** es además de técnico, organizativo, lo que implica que las medidas de seguridad afectan además de a lo técnico a las personas que intervienen en el tratamiento de los datos así como a la organización de las mismas. Así destacar la Ley canadiense en la que se hace referencia a medidas físicas, organizativas y técnicas. Es necesario recordar que también son medidas de carácter jurídico, en el sentido de que vienen determinadas o reguladas por una norma legal.

3.- **Grados de medidas de seguridad:** tanto el Reglamento de Medidas de Seguridad que desarrolla las previsiones contenidas en la LOPD en este punto, como la Ley canadiense hacen referencia a distintos niveles de medidas de seguridad. El Reglamento de Medidas de Seguridad distingue tres niveles de medidas de seguridad y la Ley canadiense dispone que dependiendo de los datos tratados, cuanto éstos sean más

sensibles, habrá de adoptarse un nivel de medidas de seguridad más alto.

Desde el punto de vista de la normativa mexicana en la materia, la obligación de los responsables de adoptar las medidas de seguridad tiene por objeto garantizar la privacidad de los individuos ya que, al asegurar la confidencialidad e integridad de la información, se protege frente a intromisiones no deseadas por parte de terceros o como consecuencia de contingencias naturales. En concreto, en la fracción VI del artículo 20 se establece la obligación de quienes tengan sistemas de datos personales de:

> *"Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado."*

Los Lineamientos en protección de datos que se refieren a la seguridad de los datos son los 9, 11 y 12 y 32 a 39 que disponen respecto del principio de seguridad de datos que:

> *"9. No se deberán registrar datos personales en archivos o sistemas que no reúnan las condiciones técnicas de integridad y seguridad conforme a estos Lineamientos y las demás disposiciones aplicables."*

El Lineamiento 11 por su parte recoge la necesidad de que las medidas de seguridad que se adopten se reflejen en una documentación que además de acreditar su existencia pueda ser puesta a disposición del Instituto cuando lo solicite. Dice así:

> *"Las dependencias y entidades deberán proporcionar al Instituto la información que este requiera y permitir a sus funcionarios visitas y acceso a los lugares en los que se encuentran y operan los sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la Ley y estos Lineamientos."*

En el Lineamiento 12 se dice que:

> *"No se deberán registrar datos personales en archivos o sistemas que no reúnan las condiciones técnicas de integridad y seguridad conforme a estos Lineamientos y las demás disposiciones aplicables.*
>
> *Las dependencias y entidades deberán proporcionar al Instituto la información que este requiera y permitir a sus funcionarios visitas y acceso a los lugares en los que se encuentran y operan los sistemas de datos personales, así como poner a su disposición*

la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la Ley y estos Lineamientos.

Las dependencias y entidades deberán establecer: la organización, instalación y equipamiento necesarios para asegurar el funcionamiento de sus sistemas y garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Las disposiciones y planes que las dependencias y entidades emitan respecto al artículo anterior, deberán incluir procedimientos y estándares mínimos de seguridad en los equipos, comunicaciones, redes y operación de los sistemas."

Y en el Lineamiento 13 que:

"Se deberá contar con planes de contingencia vigentes y probados que garanticen la continuidad del funcionamiento de los sistemas de datos personales."

Por su parte los Lineamientos 32 a 39[26] entrar a detallar medidas concretas de seguridad que son aplicables a los sistemas de datos de carácter personal y de entre ellos destacamos las siguientes apreciaciones:

[26] Lineamiento 32: *Con relación a las instalaciones y equipo de cómputo se deberá contemplar:*

- ***I.*** *Asignar espacio seguro y cómodo para la operación de los sistemas de datos personales;*
- ***II.*** *Proteger y controlar el acceso físico a las instalaciones donde se encuentra el equipamiento que soporta la operación de los sistemas de datos personales;*
- ***III.*** *Contar con al menos dos lugares distintos para almacenar medios de respaldo que reúnan condiciones de seguridad;*
- ***IV.*** *Realizar procedimientos de control y registro de asignación y baja de los equipos de cómputo a los usuarios que procesan datos personales, considerando al menos las siguientes actividades:*
  - *a) Verificar y tomar nota del contenido del equipo para facilitar la rendición de cuentas del usuario que lo recibe o lo deja;*
  - *b) Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto en hardware como en software.*
- ***V.*** *Implantar procedimientos para control de asignación y renovación de claves de acceso a equipos de cómputo y a los sistemas de datos personales;*
- ***VI.*** *Implantar medidas de seguridad para el uso de los dispositivos de salida, así como para evitar el retiro no autorizado de medios con información;*
- ***VII.*** *En el caso de disponibilidad crítica de datos, instalar y mantener el equipamiento de cómputo, eléctrico y telecomunicaciones con la redundancia necesaria. Además, realizar respaldos en línea para garantizar la continuidad de la operación.*

Lineamiento 33: *En relación a los aspectos de seguridad al utilizar la red (local, virtual, Intranet y/o inalámbrica) y las comunicaciones donde se transmitan datos personales, es necesario establecer:*

- ***I.*** *Procedimientos de control de acceso a la red que consideren perfiles de usuarios o grupos para el acceso a las funciones y programas de los sistemas de datos personales;*
- ***II.*** *Procesos de encriptamiento de archivos que garanticen la confidencialidad de la información durante la transmisión de datos personales;*
- ***III.*** *Mecanismos de control para detección, rastreo y eliminación de accesos indebidos internos o externos a la red y, de ser posible, el registro de los actos cometidos derivados de accesos no autorizados;*

Lineamiento 34: *El responsable del tratamiento de datos personales elaborará e implantará la seguridad de estos mediante un documento de observancia obligatoria para los servidores públicos con acceso autorizado a los datos personales y a los sistemas de información.*

Lineamiento 35: *El documento mencionado en el lineamiento anterior deberá contener, como mínimo, los siguientes aspectos:*

a) *Especificación detallada de los datos personales protegidos y el ámbito de aplicación del documento.*
b) *Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos.*
c) *Funciones y obligaciones de los servidores públicos autorizados para el tratamiento de datos personales.*
d) *Estructura y descripción de los sistemas de datos personales.*
e) *Procedimiento de notificación, gestión y respuesta ante las incidencias.*
f) *Procedimientos de realización de copias de respaldo y de recuperación de los datos y*
g) *Las medidas necesarias para desechar o reutilizar un sistema de datos personales.*

El contenido del documento deberá actualizarse a las disposiciones vigentes en materia de seguridad de los datos personales.
Lineamiento 36: *Únicamente los servidores públicos autorizados en el documento de seguridad podrán tener acceso a los espacios físicos donde se encuentren ubicados los sistemas de datos personales.*

Lineamiento 37: *El responsable del tratamiento de datos personales deberá llevar un registro de incidencias en el que se consignen, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.*

Lineamiento 38: *Para cada acceso deberán guardarse, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.*

Lineamiento 39: *En las actividades relacionadas con la operación: acceso, actualización, respaldo y recuperación de información de datos personales, se deberá considerar:*

I. *Contar con manuales de procedimientos y funciones para la operación de datos personales que deberán observar obligatoriamente los usuarios de los sistemas;*
II. *Establecer procedimientos para generar, asignar, distribuir, modificar y almacenar claves de acceso para la operación del sistema, que garantice la confidencialidad e integridad de los datos personales;*
III. *Llevar control y registros en bitácoras del sistema considerando la operación cotidiana, respaldos, usuarios, incidencias y accesos, así como, la comunicación de datos y sus destinatarios;*
IV. *Garantizar que el personal encargado del tratamiento de datos personales, sólo tenga acceso a las funciones autorizadas del sistema, según su perfil de usuario;*
V. *Aplicar procedimientos de respaldos de bases de datos y realizar pruebas periódicas de restauración;*
VI. *Llevar control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales;*
VII. *Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de las bases de datos de los sistemas de datos personales;*
VIII. *Garantizar que durante la comunicación de datos personales y transporte de los soportes de almacenamiento, los datos no sean leídos, copiados, alterados o suprimidos sin autorización;*
IX. *Aplicar procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales;*

El Lineamiento 34 refuerza la necesidad de la existencia de una documentación que recoja las medidas de seguridad que se adopten, mientras que el Lineamiento 35 hace referencia al contenido de esa documentación.

Se reúnen un conjunto de medidas de seguridad que hacen referencia a las instalaciones y equipos de cómputo, así en el Lineamiento 32; a la seguridad al utilizar la red y las comunicaciones donde se transmitan datos personales (Lineamiento 33); al control de acceso físico en el Lineamiento 36; a la existencia de un registro de incidencias (en Lineamiento 37); a la existencia de un registro de accesos (Lineamiento 38), y en el Lineamiento 39 a las copias de respaldo y de recuperación de datos.

Sin entrar en el fondo de cada una de las medidas de seguridad exigidas en los Lineamientos, por no ser todavía una norma publicada, recomendamos observar cómo a diferencia de lo que sucede en algunas de las legislaciones analizadas, como son la de España y la de Canadá, no se establecen diferencias de niveles en las medidas de seguridad, y, por el contrario, se fijan unas medidas de seguridad aplicables a cualquier sistemas de datos personales que contenga datos de carácter personal independientemente del tipo de datos que sean.

Sin perjuicio de lo dispuesto en este Proyecto de Lineamientos, es necesario tener en consideración que el IFAI tenía también un Anteproyecto de Lineamientos generales para el manejo, mantenimiento, seguridad y protección de los datos personales que están en posesión de las dependencias y entidades, por lo que será necesario analizar el principio de medidas de seguridad en atención a los Lineamientos que finalmente se aprueben y que podrían ser un claro referente para una regulación específica, en esta materia de seguridad, de la protección de datos de carácter personal en México.

La distinción en niveles de medidas de seguridad viene motivada por la propia naturaleza de los datos que se tratan y por la información que respecto de su

---

X. *Programar auditorias internas a efecto de verificar que se está cumpliendo con las medidas técnicas y administrativas planteadas en estos Lineamientos;*

XI. *En los casos en que la operación sea externa, realizar auditorias periódicas al proveedor del servicio, con el objeto de: verificar que se respete la confidencialidad, disponibilidad e integridad de los datos personales; revisar que el tratamiento se está realizando conforme a los acuerdos establecidos; así como, que se cumplan los estándares de seguridad planteados en estos Lineamientos;*

XII. *Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos.*

titular contienen, y, en este sentido, hemos ya visto cómo la propia Directiva 95/46/CE recoge bajo el título "Categorías especiales de datos", datos que contienen una información especialmente sensible de sus titulares y para los que exige un tratamiento específico.

Conclusiones: la seguridad de los datos personales es otro los principios que tiene que estar presente en el tratamiento de los datos personales, refiriéndose ésta a la necesidad de que quienes traten datos de carácter personal, ya sea el responsable del sistema de datos personales o el encargado del tratamiento, adopten medidas de índole técnica y organizativas necesarias para garantizar la integridad y confidencialidad de la información.

Estas medidas de seguridad, cuya adopción se prevé en todas las normas internacionales que son objeto de este análisis, es recomendable que se establezcan en atención a la naturaleza de los datos personales que sean objeto de tratamiento. Así, pueden determinarse varios niveles según la naturaleza de los datos personales que sean objeto de tratamiento, de manera que los datos que requieran una especial protección tendrán que tener también medidas de seguridad de un nivel superior, y viceversa, los que tengan menos peligro, en cuanto a su confidencialidad e integridad, requerirán un menor establecimiento de medidas de seguridad.

Por último, si bien en México existe un Anteproyecto de Lineamientos y un Proyecto de Lineamientos, sería conveniente que la regulación que se establezca al respecto se haga partiendo de las previsiones que se contengan en la normativa específica sobre protección de datos, si bien toda la regulación que pueda establecerse en este momento sería válida o, al menos, serviría para recabar una experiencia práctica en la materia que permitiera a los responsables de sistemas de datos personales o a los encargados del tratamiento cumplir con las disposiciones normativas que se establezcan.

2.6. Principio de confidencialidad/deber de secreto

Respecto del deber de secreto es importante destacar que es un deber que debe observarse por toda persona que tenga acceso a los datos, durante todo el tiempo que dure el tratamiento y aun después de que finalice el mismo.

Se trata de un deber de secreto específico, independiente de la obligación de secreto que tengan las personas que traten datos de carácter personal, por ejemplo, la obligación de confidencialidad de los abogados y médicos o de las obligaciones específicas de los empleados de cumplir con las obligaciones

contractuales de confidencialidad que, en general, se imponen en los contratos de trabajo o de prestación de servicios.

En definitiva, el deber de secreto busca garantizar que quienes traten datos de carácter personal en el desarrollo de sus funciones los guarden y garanticen el secreto sobre los mismos.

En la Directiva 95/46/CE:

La Directiva 95/46/CE no recoge referencia expresa al deber de secreto, si bien hace referencia a la necesidad de respetar la confidencialidad de la información cuando en su art. 16 dispone:

> *"Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal."*

En las normas nacionales:

LOPD	LEY Nº 25326	PIPED Act
Deber de secreto		
Art. 10	**Arts. 10 y 40**	
El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.	1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública." Art. 40: 1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística. 2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las	1) Subject to subsections (2) to (5), 13(3) and 19(1), the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part.

	excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad.	

En cuanto al deber de secreto, es necesario tener presente que la LAI no establece expresamente este deber de secreto u obligación similar para quienes tratan datos de carácter personal.

Conclusiones: en el desarrollo de una norma que regule la protección de datos personales, y sin perjuicio de las obligaciones que otras normas del ordenamiento jurídico puedan establecer sobre la obligación de secreto o confidencialidad que puedan tener determinadas profesiones, como la de abogado o médico, es necesario incluir este principio de manera que tanto el responsable del sistema de información como quienes traten datos de carácter personal tengan una obligación de secreto sobre estos datos, incluso una vez que su relación con el responsable del sistema de datos personales finalice.

2.7. Comunicación de datos a terceros

La cesión de datos es un punto conflictivo cuando se trata de proteger la llamada "privacidad"; de una parte, porque cediendo los datos a otros sistemas de datos personales se posibilita el cruce de los mismos, aplicando con toda intensidad las posibilidades de tratamiento de la información que posee la informática y, de otra parte, porque la propia cesión facilita la utilización de los datos para un uso que no es el mismo para el que se habían recabado.

Ni el Convenio 108, ni la Directiva 95/46/CE dedican un artículo a la comunicación de datos a un tercero.

La Directiva 95/46/CE define, como hemos comprobado en un apartado anterior en este Informe, la figura del destinatario de los datos y hace referencia en distintas ocasiones a la comunicación de datos a un tercero lo que da cabida al estudio de la comunicación o cesión de datos a un tercero por el responsable del sistema de datos personales.

Respecto a las legislaciones que analizamos debemos distinguir varias cuestiones acerca de la comunicación de datos cuales son:

1. **Regla general de la comunicación:**

En primer lugar, para entrar a analizar la regla general que las Leyes de Protección de Datos de España, Argentina y Canadá establecen, exponemos en la siguiente tabla los artículos referentes a la misma que disponen:

LOPD	LEY Nº 25326.	PIPED Act
Comunicación de datos: Regla general		
Art. 11.1	**Art. 11**	**Clause 4.3 of the SHEDULE 1.**
Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.	Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.	The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Del análisis de la tabla comparativa deducimos cómo la regla general en materia de comunicación o cesión de datos es la de la necesidad de consentimiento del interesado o titular de los datos para poder proceder a la comunicación de sus datos de carácter personal a un tercero, salvo que la Ley prevea otra cosa, o nos encontremos ante alguna de las excepciones que se puedan prever.

Es, por tanto, necesario el consentimiento del titular de los datos, y en España y Argentina se exige que este consentimiento sea un consentimiento concreto para un cesionario también específico, determinando con claridad la finalidad de la cesión que se consiente.

A pesar de requerir el consentimiento, ninguna de las normas que analizamos detalla qué forma debe revestir este consentimiento, lo que nos lleva a detenernos un momento en el análisis de qué formas puede revestir ese consentimiento. No se indica que este consentimiento deba ser escrito, ni revestir un formalismo determinado, de donde podemos deducir que puede ser tácito[27], siempre que podamos de él determinar con claridad la finalidad de

[27] Para no provocar errores, diremos en que el consentimiento tácito es válido siempre que la ley no diga otra cosa (como es el caso de los datos especialmente protegidos, que analizaremos después), pero no es recomendable el consentimiento tácito por las dificultades de prueba que tiene. Por lo tanto nuestra

la cesión que se consiente. No obstante, sí encontramos alguna referencia en la que la comunicación exige una forma determinada, como puede ser en la LOPD la comunicación de datos referidos al origen racial, a la salud y a la vida sexual, que sólo podrán ser cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente, como consecuencia del especial tratamiento que estas categorías de datos, como hemos visto, requieren.

Analizado lo anterior, cabe destacar que la normativa mexicana referente a la protección de datos indica, en el artículo 21 de la LAI, respecto de la comunicación de datos lo siguiente:

> *"Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información."*

Los Lineamientos sobre protección de datos, en su Lineamiento 22, hace referencia en igual sentido a la necesidad de consentimiento expreso y por escrito o por medio de autenticación similar para la comunicación de datos.

Por su parte el Lineamiento 23, añade:

> *"Los titulares de los datos podrán otorgar y revocar su autorización para que se difundan, distribuyan o comercialicen sus datos personales a terceros.*
>
> *La autorización deberá ser por escrito con firma autógrafa y anexando copia de identificación oficial del titular de los datos."*

De esta forma la regla general en materia de comunicación de datos es la de la exigencia de consentimiento expreso por escrito o por medio de autenticación similar como regla general, lo que presenta la ventaja de la prueba del consentimiento, de manera que el responsable del tratamiento o sistema de datos personales encuentra en ese documento constancia del consentimiento requerido. Sin embargo, en nuestra opinión, cerrar toda posibilidad a que ese consentimiento pueda ser válido cuando sea tácito, puede llegar a entorpecer el tráfico jurídico en algunas ocasiones. Si bien es recomendable en todo caso el que el responsable del tratamiento tenga prueba del consentimiento, reflejar

recomendación es la de acudir al consentimiento tácito solamente en los casos en que sea absolutamente necesario.

en una norma que este consentimiento sólo pueda prestarse como expreso y por escrito o medio de autenticación equivalente podría resultar, aparte de una garantía, una exigencia poco práctica.

Destacar también cómo dentro del concepto de comunicación de los datos queda incluida la difusión, distribución o comercialización de los datos personales.

2. Excepciones a la regla general.

Siendo la regla general para la comunicación de datos, como venimos analizando, la necesidad de consentimiento, todas las normas incluyen una relación de excepciones que se recogen a continuación:

LOPD	LEY Nº 25326.	PIPED Act
Comunicación de datos: Excepciones		
Art. 11.2 y 6	**Art. 11**	**7.3**
2. No será necesario el consentimiento cuando: a) está autorizada en una ley. b)se trate de datos recogidos de fuentes accesibles al público. c) el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines	El consentimiento no es exigido cuando: a) Así lo disponga una ley; b) En los supuestos previstos en el artículo 5° inciso 2[28]; c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables	For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization; (b) for the purpose of collecting a debt owed by the individual to the organization; (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records; (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national

[28] El art. 5.2 de la Ley nº 25326 recoge las excepciones a la necesidad de consentimiento para el tratamiento de datos de carácter personal.

históricos, estadísticos o científicos. f) la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. 6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.		security, the defence of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province; (d) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization (i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or (ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs; (e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure; (f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed; (g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation; (h) made after the earlier of

		(i) one hundred years after the record containing the information was created, and (ii) twenty years after the death of the individual whom the information is about; (h.1) of information that is publicly available and is specified by the regulations; (h.2) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or (i) required by law.

La LAI por su parte, recoge en el artículo 22 un conjunto de excepciones para la necesidad de ese consentimiento diciendo:

"No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:
I. (Se deroga)[29].
II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
IV. Cuando exista una orden judicial;
V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y
VI. En los demás casos que establezcan las leyes."

Conclusiones: la comunicación de datos en las normas analizadas, si bien tiene como regla general el consentimiento del titular, incluso en la normativa mexicana de modo expreso, encuentra determinadas excepciones a la necesidad de dicho consentimiento. Si bien las excepciones son necesarias, hay que tener en cuenta que el principio del consentimiento es el eje alrededor del que gira la normativa en protección de datos, y, en este sentido, representa una garantía sustancial para el individuo. De otro lado, las excepciones coinciden en la mayor parte de las normas, se pueden encontrar también particularidades locales, como la referida a los notarios en Québec.

[29] En este sentido, puede verse la nota al pie número 19, en la que se incluye el texto derogado.

3. Revocabilidad del consentimiento.

Al igual que en el principio de consentimiento, el consentimiento necesario para la cesión o comunicación de datos, salvo en las excepciones previstas en la ley, es en todo caso revocable por el titular de los datos. Así se recoge en las tres legislaciones analizadas, como se refleja en la tabla que sigue:

LOPD	LEY Nº 25.326	PIPED Act
Comunicación de datos: Revocabilidad del consentimiento.		
Art. 11	**Art. 11**	**Clause 4.3.8 of the SHEDULE 1.**
4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.	El consentimiento para la cesión es revocable.	An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal
3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.		

Respecto de la revocabilidad, podemos destacar que la LOPD, cuando trata del principio de consentimiento en su artículo 6, como hemos analizado en el apartado dedicado al mismo, indica expresamente que la revocación del consentimiento no tiene carácter retroactivo.

Por su parte, en México, el Lineamiento 23, como hemos señalado anteriormente, también recoge la posibilidad de revocar ese consentimiento prestado para la comunicación de datos:

> *"Los titulares de los datos podrán otorgar y revocar su autorización para que se difundan, distribuyan o comercialicen sus datos personales a terceros.*
> *La autorización deberá ser por escrito con firma autógrafa y anexando copia de identificación oficial del titular de los datos."*

4. Responsabilidad del cesionario de los datos.

En la comunicación de datos, por definición existe un tercero destinatario de los datos (el cesionario) que queda obligado por la comunicación a observar

respecto de los datos de carácter personal las reglas establecidas al efecto por la normativa. Así se refleja en las normas española y argentina sobre protección de datos como se recoge en la tabla que sigue.

LOPD	LEY Nº 25326.	PIPED Act
Comunicación de datos: Responsabilidad del cesionario de los datos		
Art. 11	**Art. 11**	
Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.	El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.	

Conviene resaltar, en este punto, que la norma argentina da un paso más, y establece una responsabilidad solidaria y conjunta entre los dos responsables de sistemas de datos peronales, lo que *de facto* les une en dicha responsabilidad, mientras que la española distingue entre las responsabilidades de cada uno, que les serán exigidas en relación a sus actuaciones independientes.

2.8. Acceso a los datos por terceros

Por último, tiene que prestarse atención al principio de acceso a los datos por terceros, siendo el acceso a los datos por terceros habitual en el desarrollo de la actividad de cualquier entidad, pública o privada, ya que en determinadas ocasiones el responsable del sistema de datos personales decide externalizar algunas actividades, tales como por ejemplo, mailings, introducción de datos, etc., y ello por diversas razones técnicas o económicas. No obstante, el acceso a los datos de los que es responsable el titular del sistema de datos tiene que reunir las garantías que exige la normativa sobre protección de datos, en aras a garantizar la privacidad de los interesados cuyos datos son objeto de tratamiento.

Como decíamos, la práctica diaria de las entidades en cuanto al tratamiento de datos de carácter personal y, expresado en otros términos, la necesidad y utilización real de esta figura de acceso a los datos por un tercero, debe permitir el acceso a los datos, normalmente con una referencia en el contrato que regule dicha prestación, y la consiguiente autorización por el responsable del sistema de datos personales, a aquellas personas a las que se podrá encargar un tratamiento específico.

El acceso a los datos por terceros, o también conocido como la prestación de servicios por cuenta de un tercero, se recoge en las legislaciones que analizamos como una figura distinta de la comunicación de datos, siendo necesario recordar que expresamente, por ejemplo en la ley española, se establece que *"no será considerada comunicación de datos"* tal y como comienza diciendo el artículo 12 de la LOPD. Esta figura del acceso a los datos por terceros nos lleva a analizar la figura del encargado del tratamiento.

En la Directiva 95/46/CE:

En este sentido la Directiva 95/46/CE define al encargado del tratamiento como:

> *"La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento."*

Asimismo, otra de las referencias que la citada Directiva realiza sobre esta figura es la relativa a la obligación del encargado del tratamiento de observar las medidas de seguridad necesarias para que los datos que trata por cuenta del responsable del tratamiento estén debidamente protegidos, y de este modo el apartado 2 del artículo 17 del citado texto normativo dispone:

> *"2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas."*

Y, a continuación, indica respecto del contrato que regule la prestación del servicio por el tercero que accede a los datos personales, que:

> *"3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:*
>
> *- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable deltratamiento;*
> *- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.*
>
> *4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente."*

En las normas nacionales:

Por su parte la normativa sobre protección de datos que venimos analizando dispone a este respecto lo siguiente:

LOPD	LEY Nº 25326.	PIPED Act
Acceso a los datos por terceros		
Art. 12	**Art. 25**	**Clause 4.1.3.of the SHEDULE 1.**
No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.	1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.	An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.		
En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.		
Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.	Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.	
En el caso de que el encargado		

del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.		

Del análisis anterior se desprende la recomendación de que los tratamientos que se realicen por cuenta de terceros figuren en un contrato que conste por escrito o *"en cualquier otra forma que permita acreditar su celebración y contenido"*, tal y como reza el artículo 12 de la LOPD analizado, en el que se establezcan todas las características del tratamiento y se destaque expresamente que no se puedan comunicar estos datos, ni tan siquiera para su conservación, a terceros, con lo que queda totalmente prohibida la subcontratación. En este mismo sentido, dice la PIPED Act "*The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party*"

La LAI, por su parte, establece (fracción V de su artículo 22) que no será necesario el consentimiento del interesado para proporcionar sus datos a un tercero al que se contrate para la prestación de un servicio que requiera el tratamiento de datos personales.

Se trata por tanto de la regulación del acceso a los datos por un tercero como una excepción a la necesidad de consentimiento expreso y por escrito o por un medio de autenticación equivalente.

Por su parte los Lineamientos disponen a este respecto que:

> Lineamiento 21: *"Cuando exista la contratación de un tercero para que realice el tratamiento de datos personales, se le deberán exigir, al menos, las medidas de seguridad y confidencialidad establecidas en estos lineamientos y en la reglamentación propia de las dependencias y entidades."*

Antes de seguir analizando los Lineamientos que se refieren, en nuestra opinión, a la figura que la Directiva contempla como encargado del tratamiento y por tanto como supuesto de acceso a los datos por un tercero, debemos señalar como cuestión previa que el Lineamiento 2º define *transmisión* como: *"Toda cesión de datos personales realizada de una dependencia o entidad a otra."* De esta definición, y a efectos de las recomendaciones del presente informe, deducimos que se está utilizando el término transmisión como equivalente a cesión o comunicación de datosqué queremos decir aquí???

Porque si es eso, tendríamos que decir que sería conveniente distinguir cesión de lo que no lo es. Aquí tengo yo también un poco de despiste…cuidado! Qué es lo que buscamos?

Partiendo de esta premisa diremos que lo establecido a este respecto en el Lineamiento 25[30] hace referencia a la necesidad de que la *transmisión* de datos de carácter personal se encuentre reflejada en un convenio en el que se indiquen los siguientes extremos:

> *"I. Identificación del transmisor y el destinatario de los datos;*
> *II. Justificación y finalidad de la transmisión, así como los datos que son objeto de la transferencia;*
> *III. Compromiso del destinatario a adoptar las medidas de seguridad en materia de protección de datos personales;*
> *IV. Garantía de que el titular de los datos podrá ejercitar los derechos de acceso, modificación y corrección, tanto ante el transmisor como ante el destinatario de los datos; y*
> *V. Obligación de que una vez concluida la vigencia del convenio, los datos personales deberán ser destruidos o devueltos al transmisor, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transmisión."*

Otros Lineamientos que se refieren a esta materia son:

> Lineamiento 26*: "Los datos personales transmitidos sólo podrán ser utilizados para las finalidades para las que fueron recabados por el transmisor."*
>
> Lineamiento 27: *"Los datos personales objeto de la transmisión, no podrán ser divulgados en virtud de su carácter confidencial."*
>
> Lineamiento 28: *"Se suspenderá temporalmente la transmisión de datos hacia un sujeto obligado o entre dependencias y entidades cuando se haya declarado la existencia de un nivel inadecuado de protección de datos, declaración que procederá cuando concurra alguna de las circunstancias siguientes:*

[30] *"En las transmisiones de datos personales realizadas por las dependencias y entidades, será necesario la formalización de un convenio celebrado entre el transmisor y el destinatario de los datos, en el que consten las garantías de protección de la vida privada de los titulares y del ejercicio de sus respectivos derechos."*

El convenio citado deberá contener, al menos, las siguientes características:

I. Identificación del transmisor y el destinatario de los datos;
II. Justificación y finalidad de la transmisión, así como los datos que son objeto de la transferencia;
III. Compromiso del destinatario a adoptar las medidas de seguridad en materia de protección de datos personales;
IV. Garantía de que el titular de los datos podrá ejercitar los derechos de acceso, modificación y corrección, tanto ante el transmisor como ante el destinatario de los datos; y
V. Obligación de que una vez concluida la vigencia del convenio, los datos personales deberán ser destruidos o devueltos al transmisor, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transmisión."

I. Que el destinatario haya vulnerado las normas de protección de datos.
II. Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad o dependencia destinataria de la transmisión. En este caso se podrá suspender la transmisión cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los titulares de los datos."

Lineamiento 29: *"El nivel de protección adecuado será declarado por el IFAI tomando en consideración las medidas adoptadas y la vulnerabilidad de las bases de datos."*

Lineamiento 30 *"Las dependencias y entidades deberán presentar un informe semestral al Instituto sobre las transmisiones realizadas y el tratamiento de los datos personales objeto de la transmisión para asegurar el efectivo cumplimiento de las normas que garanticen la protección de los datos personales."*

Lineamiento 31 *"El informe deberá contener, entre otros, la siguiente información:*

- *Sistema de datos personales transmitido*
- *Transmisor*
- *Destinatario*
- *Objeto de la transmisión*
- *Duración por la que se realizará la operación."*

La regulación de la transmisión expuesta si bien puede coincidir con la figura del encargado del tratamiento en la Directiva 95/46/CE, al utilizar el término de comunicación o cesión de datos vendría a complicar, en nuestra opinión, la diferencia entre las dos figuras, y, en definitiva, el tráfico jurídico y la necesidad o interés de que terceros puedan acceder a información para realizar tratamientos por cuenta de los responsables de los sistemas de datos que les ayuden en la gestión de la información en las entidades.

Sin embargo, si prescindiéramos de la clara significación que en protección de datos tiene el término cesión, y sus implicaciones, y entendemos esta regulación referida al acceso a los datos por un tercero, entonces sí que entendemos como necesarias todas las previsiones realizadas al respecto, que coinciden por otro lado, con la regulación más o menos detallada que realizan de este supuesto las normas analizadas.

Como hemos analizado, tanto en la Directiva europea como en la normativa referida se contempla la figura del encargado del tratamiento como la que surge cuando resulta necesario para prestar un servicio al responsable del

tratamiento, y no coincide, es más es muy diferente, con una comunicación de datos, puesto que el encargado del tratamiento no es responsable del tratamiento de los datos, en tanto se limite a las instrucciones dadas por el responsable del tratamiento al que presta el servicio, y procede a realizar un tratamiento de datos por un encargo concreto y para una finalidad concreta y determinada y está legitimado para el tratamiento de datos en tanto en cuanto y mientras cumpla con ese encargo.

Conclusiones: en el tratamiento de datos de carácter personal puede intervenir, además del responsable del sistema de datos personales, un tercero, al que en la normativa examinada se conoce generalmente como "encargado del tratamiento", que accede a los datos de carácter personal de los que aquél es responsable para prestarle algún servicio. Es conveniente, y además uno de los requisitos más comunes establecidos en las normas que venimos analizando, que esta prestación de servicios quede regulada en un contrato, que conste por escrito o en alguna otra forma que permita acreditar su celebración y contenido, en el que se indiquen las obligaciones que tendrá que cumplir el encargado del tratamiento en el tratamiento de los datos de carácter personal.

En concreto, si atendemos a los requisitos del artículo 12 de la LOPD, que es quizá la norma que más los detalla, el contrato tendrá que contener las instrucciones del responsable del sistema de datos personales para el tratamiento de datos de carácter personal por el encargado, el compromiso de este último de adoptar medidas de seguridad, que no utilizará los datos con un fin distinto al previsto en el contrato ni los comunicará, ni siquiera para su conservación, a terceras personas, y que una vez que finalice el contrato el encargado tendrá que devolver los datos personales al responsable, así como la documentación o soportes en los que se contengan datos o, en su caso, destruirlos.

3. DERECHOS DE LOS INTERESADOS

Para conocer los derechos de los titulares de datos de carácter personal, también denominados en las normas sobre protección de datos como interesados o afectados, debemos partir de los principios que en esta materia hemos analizado en un apartado anterior de este informe. Estos principios se quedarían en meras declaraciones teóricas si no tuvieran a su lado la posibilidad del ejercicio de unos derechos por el ciudadano que dieran contenido y efectividad práctica a esos principios.

De esta forma tenemos que decir que el titular del sistema de datos personales o del tratamiento no cumple solamente con tratar los datos de carácter personal respetando todos los principios recogidos en la norma si no que, además, es necesario que permita y facilite el ejercicio de los derechos por el interesado. Esto supone que los derechos reconocidos en la Ley a los interesados se conviertan en un instrumento propicio para controlar el tratamiento que, de sus datos personales, haga el responsable del sistema de datos personales, y, en su caso, instarle a modificar o cancelar aquellos datos cuyo tratamiento no resulte procedente, así como a conocer qué información se está tratando sobre su persona.

Dicho de otra forma, la obligación de atender al ejercicio de los derechos lleva a que el responsable del sistema de datos personales deba estructurar un procedimiento lógico-administrativo que facilite el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos.

Comenzamos, por tanto, la exposición de los derechos de las personas que implican una obligación para el responsable del sistema de datos personales de tomar unas medidas y establecer unos procedimientos para su ejercicio en casi todos los casos y en otros, los menos, a conocerlos.

3.1. Derecho de acceso

El primer derecho que vamos a analizar es el derecho de acceso que faculta a los titulares de los datos para solicitar al responsable del sistema de datos personales información relativa al tratamiento de sus datos personales, pudiendo conocer qué datos tiene sobre él y a quiénes se van a comunicar.

En el Convenio 108:

La letra b) del artículo 8 reconoce el derecho de los interesados a:

> *"obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible."*

En la Directiva 95/46/CE:

El artículo 12 de la Directiva 95/46/CE recoge el derecho de acceso disponiendo que:

> *"Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:*
>
> *a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:*
> - *la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;*
> - *la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;*
> - *el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;"*

De este modo los principios básicos que sobre este derecho de acceso establece la Directiva 95/46/CE son:

- Debe permitirse un ejercicio del derecho de acceso:
  - Libre,
  - Con una periodicidad razonable,
  - Sin retrasos, cumpliendo el plazo establecidos para la respuesta, y
  - Sin gastos excesivos para el titular de los datos.

- El derecho de acceso da derecho a conocer la existencia o inexistencia del tratamiento de datos de carácter personal, es decir, el responsable del tratamiento debe responder al ejercicio del derecho de acceso tenga o no datos de carácter personal del interesado en sus sistemas de datos de carácter personal.

- ❒ La información mínima que se debe proporcionar como respuesta al derecho de acceso debe hacer referencia a:
  - fines de dichos tratamientos,
  - las categorías de datos a que se refieran,
  - los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos,
  - el origen de los datos,
  - el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas.

- ❒ Respecto de la forma de la respuesta dispone:
  - debe proporcionarse la respuesta en forma inteligible para el titular de los datos,

Como límites al ejercicio de los derechos, el artículo 13 de la Directiva dispone lo siguiente:

"Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado;
b) la defensa;
c) la seguridad pública;
d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;
e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;
f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);
g) la protección del interesado o de los derechos y libertades de otras personas.

2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que

no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas."

En las normas nacionales:

Por su parte las legislaciones que comparativamente venimos analizando recogen el derecho de acceso del siguiente modo:

LOPD	LEY Nº 25326	PIPED Act
Derecho de acceso		
Arts. 4.6, 15 y 17.2 de la LOPD Arts. 11 y 12 del R.D. 1332/94	**Arts. 4.6, 14 y 15. Arts. 14 y 15 del Reglamento**	**Clause 9 of the Schedule 1**
Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legítimamente cancelados . (art. 4.6. LOPD)	Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.	Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. [31]
Legitimación		
11.1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.[32]	El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.	4.9.2. An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.
	En el caso de datos de personas fallecidas, deberá acreditarse el vínculo mediante la declaratoria de herederos correspondiente, o por documento fehaciente que verifique el carácter de sucesor universal del interesado."	
Forma de solicitud		
		Clause 8.
		A request under clause 4.9 of Schedule 1 must be made in writing.

[31] Esta cláusula del Anexo 1 contiene la siguiente nota. *"Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege."*

[32] El artículo 11 del Real Decreto 1332/1994 dispone en materia de legislación que *"Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero, sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el presente Real Decreto.*
Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos."

		An organization shall assist any individual who informs the organization that they need assistance in preparing a request to the organization.
Forma de respuesta		
11.2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.	La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.[33]	
Plazo de ejercicio		
11.3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.		
Coste del ejercicio del derecho de acceso		
		4.9.4. An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall

[33] El artículo 14 del Reglamento dice a este respecto: *"La solicitud a que se refiere el artículo 14, inciso 1, de la Ley Nº 25.326, no requiere de fórmulas específicas, siempre que garantice la identificación del titular. Se puede efectuar de manera directa, presentándose el interesado ante el responsable o usuario del archivo, registro, base o banco de datos, o de manera indirecta, a través de la intimación fehaciente por medio escrito que deje constancia de recepción. También pueden ser utilizados otros servicios de acceso directo o semidirecto como los medios electrónicos, las líneas telefónicas, la recepción del reclamo en pantalla u otro medio idóneo a tal fin. En cada supuesto, se podrán ofrecer preferencias de medios para conocer la respuesta requerida."*

El artículo 15 del Reglamento dispone: *"La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES elaborará un formulario modelo que facilite el derecho de acceso de los interesados. Podrán ofrecerse como medios alternativos para responder el requerimiento, los siguientes:*
a) visualización en pantalla;
b) informe escrito entregado en el domicilio del requerido;
c) informe escrito remitido al domicilio denunciado por el requirente;
d) transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información;
e) cualquier otro procedimiento que sea adecuado a la configuración e implantación material del archivo, registro, base o banco de datos, ofrecido por el responsable o usuario del mismo."

		be provided.
Plazo de contestación		
Art. 12.3 R.D. 1332/94		
El responsable del fichero resolverá entre la petición de acceso en el plazo máximo de un mes, a contar de la recepción de la solicitud. Transcurrido este plazo sin que de forma expresa se responda a la petición de acceso, éste podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992. Si la resolución fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquélla.	El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.	An organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request
		An organization may extend the time limit (a) for a maximum of thirty days if (i) meeting the time limit would unreasonably interfere with the activities of the organization, or (ii) the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet; or (b) for the period that is necessary in order to be able to convert the personal information into an alternative format. In either case, the organization shall, no later than thirty days after the date of the request, send a notice of extension to the individual, advising them of the new time limit, the reasons for extending the time limit and of their right to make a complaint to the Commissioner in respect of the extension.
		If the organization fails to respond within the time limit, the organization is deemed to have refused the request.
Forma y contenido de la respuesta al ejercicio		
La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de	1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una	4.9.1. Upon request, an organization shall inform an individual whether or not the organization holds personal

los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.	explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. 2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.[34]	information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.
Art. 13 R.D. 1332/94: La información, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso. La información comprenderá los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.	Art. 15 Decreto: El responsable o usuario del archivo, registro, base o banco de datos deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado, debiendo para ello valerse de cualquiera de los medios autorizados en el artículo 15, inciso 3, de la Ley , a opción del titular de los datos, o las preferencias que el interesado hubiere expresamente manifestado al interponer el derecho de acceso.	4.9.3. In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.
		An organization shall give access to personal information in an alternative format to an individual with a sensory disability who has a right of access to personal information under this Part and who requests that it be transmitted in the alternative format if (a) a version of the information already exists in that format; or (b) its conversion into that format is reasonable and necessary in order for the individual to be able to exercise

[34] El artículo 14 del Decreto dispone que "El derecho de acceso permitirá:
a) conocer si el titular de los datos se encuentra o no en el archivo, registro, base o banco de datos;
b) conocer todos los datos relativos a su persona que constan en el archivo;
c) solicitar información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos;
d) solicitar las finalidades para las que se recabaron;
e) conocer el destino previsto para los datos personales;
saber si el archivo está registrado conforme a las exigencias de la Ley."

		rights under this Part.
Carácter gratuito del derecho		
Art. 17.2. LOPD		
No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.	3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.	An organization may respond to an individual's request at a cost to the individual only if (a) the organization has informed the individual of the approximate cost; and (b) the individual has advised the organization that the request is not being withdrawn.
	Si se tratara de archivos o bancos de datos públicos dependientes de un organismo oficial destinados a la difusión al público en general, las condiciones para el ejercicio del derecho de acceso podrán ser propuestas por el organismo y aprobadas por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, la cual deberá asegurar que los procedimientos sugeridos no vulneren ni restrinjan en modo alguno las garantías propias de ese derecho.	An organization that responds within the time limit and refuses a request shall inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under this Part.
	4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.	Despite clause 4.5 of Schedule 1, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have.

Como se deduce del análisis de la tabla precedente las tres legislaciones analizadas cumplen con las previsiones realizadas y analizadas de la Directiva 95/46/CE al respecto, y prevén un régimen muy detallado para el ejercicio del derecho, de lo que podemos extraer fácilmente su relevancia.

Excepciones al ejercicio del derecho de acceso:

LOPD	LEY Nº 25326	PIPED Act
Derecho de acceso		
Arts. 23 y 24	**Art. 17**	**Clause 9 of the Schedule 1**
23.1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior[35] podrán denegar	1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión	Despite clause 4.9 of Schedule 1, an organization shall not give an individual access

[35] Artículo 22.2 y 3 de la LOPD: *"2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un*

el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. 2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras. 3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia Española de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.	en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado. 3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.	to personal information if doing so would likely reveal personal information about a third party. However, if the information about the third party is severable from the record containing the information about the individual, the organization shall sever the information about the third party before giving the individual access.
24.1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales.		An organization is not required to give access to personal information only if (a) the information is protected by solicitor-client privilege; (b) to do so would reveal confidential commercial information; (c) to do so could reasonably be expected to threaten the life or security of another individual; (c.1) the information was collected under

peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales."

		paragraph 7(1)(b); or (d) the information was generated in the course of a formal dispute resolution process. However, in the circumstances described in paragraph (b) or (c), if giving access to the information would reveal confidential commercial information or could reasonably be expected to threaten the life or security of another individual, as the case may be, and that information is severable from the record containing any other information for which access is requested, the organization shall give the individual access after severing.

Vista la regla general y las excepciones al ejercicio del derecho de acceso, pasemos a analizar lo que la normativa mexicana dispone al efecto:

La LAI en sus artículos 20 y 24 indica que:

"Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;"

Por su parte el artículo 24 señala:

"Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las

tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27."

El artículo 47 del Reglamento de la LAI dispone:

"Los procedimientos para acceder a los datos personales que estén en posesión de las dependencias y entidades garantizarán la protección de los derechos de los individuos, en particular, a la vida privada y a la intimidad, así como al acceso y corrección de sus datos personales, de conformidad con los lineamientos que expida el Instituto y demás disposiciones aplicables para el manejo, mantenimiento, seguridad y protección de los datos personales."

Si analizamos estos preceptos desde la perspectiva de la Directiva 95/46/CE llegamos a las siguientes conclusiones:

Requisitos del derecho de acceso	
Directiva 95/49/CE	**Normativa mexicana**
Debe permitirse un ejercicio del derecho de acceso: - Libre, - Con una periodicidad razonable,	Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales.
Sin retrasos, cumpliendo el plazo establecidos para la respuesta, y	Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud,
Sin gastos excesivos para el titular de los datos.	La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27."
El derecho de acceso da derecho a conocer la existencia o inexistencia del tratamiento de datos de carácter personal, es decir, el responsable del tratamiento debe responder al ejercicio del derecho de acceso tenga o no datos de carácter personal del interesado en sus ficheros de datos de carácter personal.	Aquélla deberá entregarle la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.
La información mínima que se debe proporcionar como respuesta al derecho de acceso debe hacer referencia a: - fines de dichos tratamientos, - las categorías de datos a que se refieran, - los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos, - el origen de los datos, - el conocimiento de la lógica utilizada en	

los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas.	
Respecto de la forma de la respuesta dispone que debe proporcionarse la respuesta en forma inteligible para el titular de los datos,	Aquélla deberá entregarle en formato comprensible para el solicitante,

Como se deduce de la tabla anterior, la normativa mexicana, a pesar de que no es específica sobre protección de datos personales, se adecua bastante en este punto a lo establecido por la Directiva 95/46/CE. Si bien queda un punto en el que la normativa mexicana podría ser algo más explícita y es el relacionado con el contenido de la información que en respuesta al ejercicio del derecho de acceso se proporciona al interesado.

3.2. Derechos de rectificación y cancelación

Los derechos de rectificación y cancelación permiten al afectado o interesado, titular de los datos, por un lado, solicitar la modificación, en los casos de que los datos sean inexactos, y cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido registrados, requerir su cancelación. Si los datos que se encuentran en un sistema de datos son inexactos, incompletos o no existiera, por el motivo que fuera, derecho a su registro por parte del titular del sistema de datos personales, el afectado podrá ejercer su derecho de rectificación o su derecho de cancelación, según corresponda.

Es así como los datos cuyo tratamiento no se ajuste a lo especificado en las normas específicas y, en particular, los datos que resulten ser inexactos o incompletos, serán rectificados o, en su caso, cancelados, debiendo comunicar el responsable del sistema de datos personales esta circunstancia, con expresa indicación de los datos rectificados o cancelados, a todos aquellos terceros a los que les hubiese transmitido la información.

Cabe destacar que, en algunas normas, se precisa que la cancelación no debe suponer automáticamente el borrado físico de los datos, sino su bloqueo. En este sentido, la cancelación no puede exigir el borrado total y absoluto de los datos, aunque sea necesario el bloqueo con todas las características de seguridad que le deban acompañar; de otra forma, nos encontraríamos ante la extraña situación de que el borrado total de los datos no permitiría atender otras obligaciones, legales o contractuales, por no existir ya rastro alguno sobre los datos, como pueden ser los requerimientos realizados por los Jueces o Tribunales, o por la propia Administración, y teniendo en cuenta, además,

que el responsable del sistema de datos personales está obligado a atender las propias responsabilidades nacidas del tratamiento de los datos.

Puede darse el caso de que la rectificación o, en su caso, la cancelación, no sea procedente y el responsable del sistema de datos personales no esté, por tanto, obligado a realizarla. En este caso pondrá en conocimiento del titular de los datos, normalmente en el mismo plazo establecido para responder al ejercicio del derecho, la no procedencia de la rectificación o la cancelación solicitada argumentando los motivos por los que no la realiza.

Si el responsable del sistema de datos hubiera transmitido a un tercero los datos que hayan sido rectificados o cancelados se le deberá comunicar a éste que se ha efectuado la rectificación o cancelación y en qué ha consistido para que actúe en consecuencia.

En este sentido, como apuntábamos, la solicitud de rectificación o cancelación no implica que el responsable del sistema de datos tenga que responder afirmativamente a la misma, sino que solamente debe atender la petición pero no está obligado a llevar a cabo la rectificación o la cancelación cuando la solicitud no sea procedente. En este aspecto difiere del derecho de acceso, que, salvo las excepciones basadas normalmente en su ejercicio repetitivo, siempre tiene que concederse lo que se pide, es decir, el acceso.

Además, por otro lado, lo anterior implica que las personas que trabajan en la organización responsable del sistema de datos personales puedan informar, en la medida que se estime necesario, sobre el procedimiento a seguir para el ejercicio de sus derechos, lo que implica que el responsable del sistema de datos debe tomar las medidas oportunas para garantizarlo. El hecho de que el personal de una entidad sepa cómo responder ante una solicitud, aunque su respuesta sólo consista en dirigir al interesado al órgano o departamento con competencia para atender al ejercicio de su derecho, es una garantía para el responsable del sistema de datos personales.

En este sentido, resulta recomendable el establecimiento de un procedimiento estandarizado, por parte del responsable del sistema de datos personal, para responder al ejercicio de los derechos.

<u>En el Convenio 108:</u>

En la letra c) del artículo 8 se establece que los interesados podrán:

"obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio".

En la Directiva 95/46/CE:

Todo esto se refleja en la Directiva 95/46/CE que recoge estos derechos en los apartados b) y c) de su artículo 12 que disponen:

Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

"b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;
c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado."

En las normas nacionales:

Por su parte las legislaciones que venimos analizando también recogen estos derechos en la forma en la que los analizamos en la tabla que sigue:

LOPD	LEY Nº 25326	PIPED Act
Derechos de rectificación y cancelación		
Art. 16	**Art. 16**	**Clause 9 of the Schedule 1**
1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.	Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.	An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. 4.9.5. When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.	2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. 3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.	
3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.	6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.	
4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.	En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.	4.9.6. When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.
	La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.	
5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.	7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.	

En la normativa mexicana encontramos una regulación, bastante similar a las que hemos analizado en la tabla que precede sobre el derecho a corregir los datos de carácter personal.

El artículo 25 de la LAI dispone:

> *"Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales.*
>
> *Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones."*

Si bien esta regulación del derecho a la corrección de los datos personales es correcta, por otro lado, quizá la materia que tratamos reclama una regulación más detallada sobre todo en aspectos concretos como los que hemos analizado por ejemplo en la norma española, como es el caso del bloqueo de los datos como resultado de la cancelación de los datos de carácter personal. En particular, esta puntualización es relevante toda vez que el responsable del tratamiento puede ser requerido por alguna responsabilidad (por ejemplo fiscales) prevista en las leyes incluso una vez finalizada su relación con el titular de los datos y para ello necesitar mantener los datos de forma que aun no teniendo ya legitimidad para tratarlos pueda usarlos como prueba durante el tiempo en el que puedan exigírsele alguna responsabilidad.

3.3. Derecho de oposición

En la Directiva 95/46/CE:

El artículo 14 de la Directiva 95/46/CE dispone que:

> *"Los Estados miembros reconocerán al interesado el derecho a:*
>
> *a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;*

b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b).”

En las normas nacionales:

LOPD	LEY Nº 25326	PIPED Act
Derecho de oposición		
Art. 6.4.	**Art.**	
En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.		

En definitiva, el derecho de oposición significa que el interesado, en aquellos casos en los que no resulte necesario su consentimiento para el tratamiento de sus datos, y siempre que una Ley no disponga lo contrario, podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos. El responsable del sistema de datos tendrá que proceder a la exclusión de los datos relativos al afectado.

3.4. Otros derechos de los titulares de los datos

La Directiva 95/46/CE, y en consecuencia la ley española, recogen, además de los derechos mencionados, otros relativos a la posibilidad del titular de los datos de impugnar las valoraciones que de él se hagan como resultado del tratamiento de sus datos de carácter personal. Asimismo, ya concretamente en la ley española, se recoge el derecho de consulta al Registro General de Protección de Datos y por último el derecho a una indemnización en el caso de que el tratamiento de sus datos se haya realizado incumpliendo las previsiones de la LOPD y le haya causado daños y perjuicios.

Derecho de consulta al Registro

Otro de los derechos previstos en las normas analizadas, y en la propia LAI, es el derecho de consulta por los interesados a un Registro público al que los responsables de los sistemas de datos personales notifiquen la existencia de los sistemas de datos de carácter personal, y que va a permitir a los interesados obtener información con el propósito de poder dirigirse a su responsable para ejercitar los derechos que la Ley le reconoce.

En el caso de la normativa mexicana es necesario atender a los Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales.

Derecho de impugnación de valoraciones

En la Directiva 95/46/CE, el artículo 15, bajo el título *Decisiones individuales automatizadas,* establece que:

> *"1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.*
> *2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:*
> *a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o*
> *b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado".*

Por su parte, en la LOPD el derecho a la impugnación de valoraciones faculta al interesado a impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Derecho a indemnización

Por último, en las normas sobre protección de datos analizadas, y en particular en la LOPD, encontramos el derecho de los interesados a recurrir a los

Tribunales con objeto de obtener una compensación, de la naturaleza que sea, en aquellos supuestos en los que el interesado haya visto vulnerado sus derechos, refiriéndonos aquí a otros bienes protegidos por el ordenamiento jurídico, tales como el derecho al honor y a la intimidad.

Conclusiones: es necesario recordar que al comienzo de este informe hemos estructurado el estudio de la protección de datos con base en un triángulo, siendo uno de sus vértices los derechos de los interesados o afectados. Esto significa que el reconocimiento en una norma sobre protección de datos de derechos a los interesados es una garantía para la protección de su privacidad, puesto que permiten garantizar la aplicación de los principios sobre la protección de datos al poder instar al responsable del sistema de protección de datos a adecuar el tratamiento de sus datos de carácter personal (de los interesados) a los requisitos que exigen dichos principios.

En concreto, los derechos de la protección de datos que se reconocen y regulan en las normas analizadas son los de: acceso, rectificación (o modificación como se denomina en la normativa mexicana), cancelación (o supresión), oposición, consulta a un Registro público, impugnación de valoraciones y a indemnización.

Es necesario asimismo resaltar que la regulación de los derechos de los ciudadanos en protección de datos conlleva que el legislador tenga que tener en consideración determinados aspectos generales que resultan transcendentes, tales como la legitimación para su ejercicio, o, incluso, aspectos concretos como que el borrado de los datos a que da lugar de la cancelación sólo puede llevarse a cabo en determinadas circunstancias, teniendo que ser previamente bloqueados y, una vez que se haya cumplido por el responsable del sistema de datos personales con las obligaciones, legales o contractuales, que tenga, suprimidos.

Por último, debe recordarse de nuevo que en México la normativa vigente regula determinados aspectos de algunos de los derechos aquí analizados, siendo conveniente tenerlos en consideración con el propósito de desarrollar posteriormente una normativa específica sobre protección de datos de carácter personal.

4. OBLIGACIONES DEL RESPONSABLE DEL SISTEMA DE DATOS

Para analizar las obligaciones del responsable del sistema de datos personales, creemos que resultaría conveniente con carácter previo retomar unas cuestiones ya tratadas en este Informe, pero que es necesario recordarlas someramente para el análisis de las obligaciones del responsable del sistema de datos personales que realizamos a continuación.

En primer lugar, debemos desatacar que para conocer las obligaciones que pueden tener los responsables de sistemas de datos o tratamientos, se requiere hacer referencias a las obligaciones que, derivadas de la protección de datos, son comunes a un responsable de un sistema de datos personales y a un encargado del tratamiento, es decir, las que debe observar un sujeto cuando realiza un tratamiento por cuenta de un tercero.

En segundo lugar debemos considerar las obligaciones que tiene el responsable del sistema de datos personales en cada una de las fases del tratamiento de datos, y que son la recogida, tratamiento y utilización y, en su caso, cesión o comunicación de datos.

Estos tres momentos deben estar siempre presentes en el estudio de cualquier aspecto de la protección de datos, tal y como venimos indicado a lo largo del Informe, y así también en materia de obligaciones del responsable del sistema de datos personales o tratamiento.

En el momento de recabar los datos, bien sea directamente del interesado o de un tercero, tiene gran importancia su licitud y lealtad (si bien, debemos indicar de nuevo que la licitud y lealtad deben estar presentes en todas las fases del tratamiento), con las características de conocimiento y, en su caso, consentimiento del afectado.

El segundo momento, el del tratamiento de los datos, que pueden ser cruzados y relacionados en forma automática junto con otros datos, buscando definir un perfil determinado del afectado que incluso él mismo llega a desconocer.

Por último, el momento de la utilización y, en su caso, comunicación a terceros de los resultados del tratamiento, conocida ésta última como "cesión o comunicación de datos", en la que, al igual que en la recogida y en el

tratamiento, se tendrá que considerar el conocimiento y consentimiento del titular.

Algunas de las obligaciones más significativas que puede tener el titular del sistema de datos son las siguientes:

- Realizar un tratamiento legal y leal de los datos.
- Inscribir los sistemas de datos personales en un Registro creado a tal efecto por el órgano de control o Autoridad en materia de protección de datos.
- Adoptar las medidas de seguridad que atendiendo a la naturaleza de los datos, al estado de la tecnología y los riesgos a que están expuestos los datos, con el propósito de garantizar la confidencialidad e integridad de la información.
- Atender el ejercicio de los derechos que se reconocen a los titulares de datos.

Habiendo dedicado otros apartados del presente Informe al principio de seguridad y a la atención del ejercicio de los derechos, realizaremos un análisis en este punto sobre las otras dos obligaciones a las que nos hemos referido.

- Realizar un tratamiento legal y leal de los datos.
- Inscribir los sistemas de datos personales en un Registro público.

4.1. Tratamiento legal y leal

Para realizar un tratamiento legal de los datos se debe cumplir con los principios que derivan de la protección de datos que son los que hemos analizado en un epígrafe anterior en el presente Informe que se refieren a la calidad de los datos, a la necesidad de consentimiento del titular de los datos para su tratamiento, a la información que se debe proporcionar al titular de los datos, a los datos especialmente protegidos, a la necesidad de adoptar determinadas medidas de seguridad, al deber de secreto y a la comunicación de datos y al acceso a los datos por terceros.

Por su parte, el tratamiento es leal[36] cuando los interesados están en condiciones de conocer la existencia de los tratamientos y, cuando los datos se

[36] En este sentido, la Directiva 95/46/CE indica en su Considerando 28 que *"todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que*

obtengan de ellos mismos o a través de terceros, cuenten con una información precisa y completa respecto a las circunstancias de dicha obtención.

El tratamiento leal de los datos también implica, la obligación del responsable del sistema de datos personales de atender el ejercicio de los derechos que se reconocen a los titulares de los datos y los cuales hemos examinado con detenimiento en otro epígrafe de este Informe.

4.2. Inscribir los sistemas de datos personales en un Registro creado a tal efecto por el Órgano de control o Autoridad en materia de protección de datos

La segunda obligación que hemos señalado, la obligación de inscribir los sistemas de datos personales en un Registro público creado al efecto, es un punto en el que difieren las obligaciones del responsable del sistema de datos personales y del encargado del tratamiento. El responsable del sistema de datos es el obligado a realizar la inscripción previa de los sistemas de datos personales cuando procede a su creación. El encargado del tratamiento no tiene sin embargo, respecto de los datos que trata para cumplir su encargo, esta obligación y tampoco asume la responsabilidad de que el sistema o sistemas de datos del responsable que le encarga el servicio estén o no inscritos en el Registro.

El establecimiento de un Registro público en el que se inscriban los sistemas de datos personales se erige como una posibilidad al establecer una regulación sobre protección de datos. La existencia de dicho Registro, que en cierto modo ya existe en la normativa mexicana cumpliendo esta función el Listado de sistemas de datos personales que lleva a cabo el IFAI, se convierte al mismo tiempo en una garantía para los interesados cuyos datos son objeto de tratamiento ya que a través del mismo podrán conocer la existencia de sistemas de datos de carácter personal de manera que podrán dirigirse a su responsable para enviarle solicitudes de ejercicio de los derechos correspondientes que la Ley les reconoce.

En cuanto a la configuración de este Registro, puede ser un órgano integrado a su vez en la Autoridad o Agencia de Protección de Datos, de carácter administrativo y cuya función es dar publicidad de la existencia de sistemas de datos personales, gestionando al mismo tiempo las notificaciones que sean

estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados".

realizadas por los responsables de los sistemas de datos personales en cuanto a su creación, modificación o supresión. Otra cuestión a tener en consideración sería el papel específico a atribuir a dicho Registro en cuanto al control a llevar a cabo sobre las notificaciones, puesto que podría configurarse como un mero control de los requisitos de la notificación, sin entrar a valorar la legalidad contenido del sistema de datos personales y correlativamente compensado con una potestad sancionadora, o un control del contenido del propio sistema de datos en el momento de proceder a su inscripción.

En la Directiva 95/46/CE:

La Directiva 95/46/CE recoge esta obligación de comunicar a una autoridad de control la existencia de sistemas de datos de carácter personal en los artículos 18 a 21, que regulan los aspectos que se indican a continuación.

El artículo 18 recoge la obligación de notificar al Registro público que se cree a tal efecto, los tratamientos de datos que se pretenden realizar. Esta notificación debe tener carácter previo a los tratamientos, el artículo referido dice así:

> *"Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos."*

Como excepciones a la regla general de la obligación de notificar la existencia de tratamientos de datos se prevén determinados supuestos que se indican en los siguientes párrafos.

Los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones:

- *cuando, para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o*
- *cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos personales que tenga por cometido, en particular:*

⇒ hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,

⇒ llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21, garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

Los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo.

Los Estados miembros podrán eximir de la obligación de notificación o disponer una simplificación de la misma respecto de los tratamientos a que se refiere la letra d) del apartado 2 del artículo 8.

Los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal o algunos de ellos sean notificados eventualmente de una forma simplificada."

En relación con el contenido de la notificación el artículo 19 de la Directiva que analizamos dispone:

"Los Estados miembros determinarán la información que debe figurar en la notificación, que será como mínimo:

a. el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante;
b. el o los objetivos del tratamiento;
c. una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento;
d. los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos;
e. las transferencias de datos previstas a países terceros;
f. una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 17 resultan adecuadas para garantizar la seguridad del tratamiento.

Los Estados miembros precisarán los procedimientos por los que se notificarán a la autoridad de control las modificaciones que afecten a la información contemplada en el apartado 1."

Se prevén en el artículo 20 de la Directiva 95/46/CE determinados supuestos que pueden ser sometidos a controles previos al tratamiento de los datos:

"Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento.

Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control

Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control

Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control.

Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías."

La Directiva también prevé en su artículo 21 la obligación de dar publicidad de los tratamientos mediante la creación de un registro público al efecto:

"Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos.

Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18.

En el registro se harán constar, como mínimo, las informaciones a las que se refieren las letras a) a e) del apartado 1 del artículo 19.

El registro podrá ser consultado por cualquier persona.

Los Estados miembros dispondrán, en lo que respecta a los tratamientos no sometidos a notificación, que los responsables del tratamiento u otro órgano designado por los Estados miembros comuniquen, en la forma adecuada, a toda persona que lo solicite, al menos las informaciones a que se refieren las letras a) a e) del apartado 1 del artículo 19.

Los Estados miembros podrán establecer que esta disposición no se aplique a los tratamientos cuyo fin único sea llevar un registro, que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo."

En las normas nacionales:

A este respecto las legislaciones de protección de datos de España, Argentina y Canadá disponen:

LOPD	LEY Nº 25326.	PIPED Act
Notificación de ficheros		
Ficheros de titularidad pública		
Art. 20	**Art. 22**	
1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente. 2. Las disposiciones de creación o de modificación de ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo. b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos. c) El procedimiento de recogida de los datos de carácter personal. d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo. e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros. f) Los órganos de las Administraciones responsables del fichero. g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición. h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible. 3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.	1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial. 2. Las disposiciones respectivas, deben indicar: a) Características y finalidad del archivo; b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas; c) Procedimiento de obtención y actualización de los datos; d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán; e) Las cesiones, transferencias o interconexiones previstas; f) Órganos responsables del archivo, precisando dependencia jerárquica en su caso; g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión. 3. En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.	
Ficheros de titularidad privada		
Art. 26	**Art. 24**	
1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección	Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto	

de Datos. 2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros. 3. Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación. 4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. 5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.	en el artículo 21.	

Antes de entrar a valorar las conclusiones que pueden extraerse de la regulación contenida en las normas que regulan la protección de datos en España, Argentina y Canadá, es conveniente tener en consideración que, a diferencia de la Directiva 95/46/CE, en la LOPD y en la Ley argentina se distingue entre sistemas de datos personales de titularidad privada y de titularidad pública, estableciéndose en ambas normas, y en especial en la LOPD, un régimen específico para cada uno de los sistemas de datos de carácter personal en atención a quién sea su titular o responsable.

Establecido lo anterior, las conclusiones que se derivan de esta obligación son que en el caso de los sistemas de datos personales de titularidad privada, ya sea una persona, física o jurídica, puede tomar la decisión de crear un sistema de datos de carácter personal cuando lo considere conveniente para sus

intereses y desarrollo de su actividad profesional o de su objeto social según el caso.

Ahora bien, una vez tomada esta decisión debe proceder, con carácter previo, a inscribir ese sistema de datos personales en el Registro público que la Autoridad de Control haya creado a tal efecto.

La inscripción de un sistema de datos personales no suele suponer la legalidad del tratamiento que se realiza dado que el Registro se limita a revisar el contenido mínimo establecido en la normativa y a pedir que se completen los datos que falten o se proceda a su subsanación.

Por su parte la normativa mexicana sobre protección de datos dispone a estos efectos en el artículo 23 de la LAI:

> *"Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales."*

Y en el artículo 48 del Reglamento de la LAI se dice así:

> *"Las dependencias y entidades que cuenten con sistemas de datos personales deberán hacer del conocimiento del Instituto y del público en general a través de sus sitios de Internet, el listado de dichos sistemas, en el cual indicarán el objeto del sistema, el tipo de datos que contiene, el uso que se les da, la unidad administrativa que lo administra y el nombre del responsable. El Instituto mantendrá un listado público actualizado de los sistemas de datos personales que sean hechos de su conocimiento."*

4.3. Atención al ejercicio de los derechos

En cuanto al ejercicio de los derechos por parte de los interesados, en el apartado de este Informe correspondiente a los derechos se ha analizado cómo tiene que responder el responsable del sistema de datos o tratamiento a su ejercicio, por lo que en aras a no resultar repetitivos en nuestra exposición nos remitimos a lo dicho anteriormente.

Conclusiones: los principios y los derechos de la protección de datos, que tienen por objeto garantizar en un ordenamiento jurídico la privacidad de los interesados, se convierten en obligaciones para los titulares de los sistemas de datos de carácter personal. En este sentido, es necesario atender a que los tratamientos de datos de carácter personal sean legales y leales, a que se

adopten medidas de seguridad, a inscribir los sistemas de datos personales en un Registro público creado al efecto y a responder al ejercicio de los derechos por los interesados.

El establecimiento de estas obligaciones, algunas de las cuales tienen que ponerse en relación con las tres fases en las que puede dividirse el tratamiento de datos de carácter personal, requiere, correlativamente, de la previsión o tipificación de infracciones con sus correspondientes sanciones para aquellos casos en los que sean incumplidas, si bien esta cuestión será tratada en el apartado correspondiente de este Informe.

Por último, es recomendable que la legislación específica que se adopte en materia de protección de datos de carácter personal establezca claramente cuáles son las obligaciones de los responsables de sistemas de datos personales, debiendo considerarse además la oportunidad de adoptar otras medidas adicionales, y no necesariamente de carácter legislativo, con el propósito de dar a conocer las obligaciones de la protección de datos y crear así una cultura social en protección de datos basada en la formación e información.

5. TRANSFERENCIA INTERNACIONAL DE DATOS

La Transferencia Internacional de Datos (TID) implica un flujo de datos personales entre diversos países haciendo surgir la necesidad de adecuar dichos tratamientos a las previsiones legales establecidas en los diversos ordenamientos jurídicos en juego, que tienen como fin garantizar al individuo, cuyos datos son objeto de tratamiento, su derecho a la protección de datos.

La realización de transferencias internacionales de datos no es supuesto extraño, sino que muy al contrario está presente en la actividad diaria de muchas entidades que tienen presencia internacional, al mismo tiempo que las Administraciones Públicas también pueden requerir o, en su caso, venir obligadas a realizar transferencias internacionales, como por ejemplo en el auxilio judicial internacional, persecución de delitos, asistencia a ciudadanos que se encuentran en otros países, etc. En este sentido, la realización de transacciones de comercio electrónico se convierte en un claro ejemplo de transferencias internacionales de datos cuando estas transacciones superan las fronteras de un país al realizarse mediante un sitio web de un prestador de servicios establecido en un tercer país, etc.

Para iniciar este epígrafe dedicado al análisis de la TID y a efectos de exponer la clasificación de la TID, y de manera esquemática, podemos decir que se pueden diferenciar con base en dos criterios:

1.º) Por el país de destino.

En función de cuál sea el país de destino, podemos diferenciar, a su vez, tres casos distintos:

1. Un país de la Unión Europea o del Espacio Económico Europeo[37].
2. Un país declarado con un nivel adecuado de protección (Suiza, Hungría[38], Canadá, entidades adheridas al Acuerdo de Puerto Seguro –Estados Unidos–, Argentina y Bailía de Guernsey e Isla de Man).
3. Un tercer país.

[37] El Espacio Económico Europeo está formado por los Estados miembros de la Unión Europea (Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Irlanda, Italia, Luxemburgo, Países Bajos, Portugal, Reino Unido, Suecia, y los adheridos recientemente, Polonia, Eslovenia, Eslovaquia, Hungría, República Checa, Estonia, Lituania, Letonia, Malta y Chipre) y Noruega, Islandia y Liechtenstein.

[38] Si bien como ya hemos indicados Hungría es un Estado miembro de la Unión Europea.

En los dos primeros casos, la TID puede realizarse del mismo modo que las comunicaciones, o en su caso prestaciones de servicios, dentro del país comunitario origen de los datos.

2.º) Por la finalidad con la que se realiza la TID.

En función de la finalidad para la que se realiza la TID, ésta puede ser a su vez:

1. Una comunicación a un tercero.
2. Un encargo o prestación de servicios.

En el análisis de la TID distinguiremos, como venimos realizando en el presente Informe la regulación que de las TID realiza la Directiva 95/46/CE y las que realizan las legislaciones que analizamos.

En el Convenio 108:

El artículo 12, relativo a los flujos transfronterizos de datos de carácter personal, establece lo siguiente:

> *"1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.*
> *2. Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte.*
> *3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2:*
> *a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente;*
> *b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo".*

A) TID en la Directiva 95/46/CE:

En materia de TID y realizando un análisis desde la perspectiva comunitaria de la Directiva 95/46/CE debemos destacar en primer lugar su regulación, en sus

artículos 25 y 26, recogiendo el primero de ellos la regla general y el artículo 26 las excepciones previstas a esa regla general.

A.1) Regla general:

El artículo 25 recoge la regla general que vamos comentando a continuación:

> *"1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado."*

Siendo por tanto la regla general la de que el país tercero al que se transfieran los datos de carácter personal desde un país sujeto al ámbito de aplicación de la Directiva 95/46/CE, deberá reunir los requisitos para ser considerado un país garantiza un nivel de protección adecuado. Para conocer cuándo un país reúne las condiciones exigidas para un nivel de protección adecuado, el apartado 2 dispone:

> *"2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países."*

El carácter adecuado del nivel de protección de datos que ofrece un país tercero se evalúa atendiendo, según lo dispuesto en el artículo 25.2 de la Directiva 95/46/CE, a:

- todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos;
- en particular, se tomará en consideración:
  - la naturaleza de los datos,
  - la finalidad y la duración del tratamiento o de los tratamientos previstos,
  - el país de origen,
  - el país de destino final,

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

Además, continúan los siguientes apartados del artículo 25 de la Directiva:

"3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión."

En este sentido destacamos, entre otras[39] y a los efectos del objeto de estudio del presente Informe, la Decisión 2002/2/CE de la Comisión, de 20 de

[39] El resto de Decisiones de la Comisión por las que se declara que terceros países tienen un nivel adecuado de protección de datos son hasta el momento:

- Decisión 2000/518/CE de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza.
- Decisión 2000/519/CE de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Hungría (Aunque actualmente esta Decisión ha perdido su fundamento puesto que recientemente Hungría ha entrado a formar parte de la Unión Europea).
- Decisión 2000/520/CE de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo Europeo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas mas frecuentes publicadas por el Departamento de Comercio de los Estados Unidos de América.
- Decisión 2003/821/CE de la Comisión, de 21 de noviembre, relativa al carácter adecuado de la protección de los datos personales en Guernsey.

diciembre de 2001, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act* y la Decisión 2003/490/CE de la Comisión, de 30 de junio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

A través de la siguiente tabla se comparan estas Decisiones:

- Decisión 2004/411/CE, de 28 de abril de 2004, de la Comisión, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man.

CANADÁ		ARGENTINA	
Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act*		Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina	
Nº	**CONSIDERANDOS**	**Nº**	**CONSIDERANDOS**
1	De conformidad con la Directiva 95/46/CE, los Estados miembros sólo permitirán la transferencia de datos personales a un país tercero si éste proporciona un nivel de protección adecuado y se cumplen en él, con anterioridad a la transferencia, las disposiciones legales que los Estados miembros aprueben en aplicación de otros preceptos de dicha Directiva.	1	De conformidad con la Directiva 95/46/CE, los Estados miembros sólo permitirán la transferencia de datos personales a un país tercero si éste proporciona un nivel de protección adecuado y se cumplen en él, con anterioridad a la transferencia, las disposiciones legales que los Estados miembros aprueben en aplicación de otros preceptos de dicha Directiva.
2	Para transferir datos personales desde los Estados miembros bastará con que la Comisión dictamine, en ejercicio de sus competencias, que un país tercero proporciona un nivel de protección adecuado.	2	La Comisión puede determinar que un país tercero garantiza un nivel de protección adecuado. En tal caso, pueden transferirse datos personales desde los Estados miembros sin que sea necesaria ninguna garantía adicional.
3	De conformidad con la Directiva 95/46/CE, el nivel de protección de los datos debe evaluarse atendiendo a todas las circunstancias que concurran en una transferencia o categoría de transferencias de datos, con respecto a unas condiciones determinadas. El Grupo de Trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, que se creó en virtud del artículo 29 de la Directiva 95/46/CE, ha dado a conocer una serie de orientaciones sobre la evaluación[40].	3	De conformidad con la Directiva 95/46/CE, el nivel de protección de los datos debe evaluarse atendiendo a todas las circunstancias que concurran en una transferencia o conjunto de transferencias de datos y estudiando con especial atención una serie de elementos relevantes para la transferencia, enumerados en el apartado 2 de su artículo 25. El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, previsto en el artículo 29 de la Directiva 95/46/CE, ha dado a conocer una serie de orientaciones sobre dicha evaluación[41].
4	Ante los diferentes enfoques sobre la protección de datos adoptados en los terceros países, tanto la evaluación de la adecuación como la ejecución de las decisiones en virtud del apartado 6 del artículo 25 de la Directiva 95/46/CE deben hacerse sin que originen, en igualdad de condiciones, una discriminación arbitraria o injustificada contra terceros países o entre ellos, ni constituyan una restricción comercial encubierta contraria a los	4	Ante los diferentes enfoques sobre la protección de datos adoptados en los terceros países, tanto la evaluación de la adecuación como la ejecución de las decisiones en virtud del apartado 6 del artículo 25 de la Directiva 95/46/CE deben hacerse sin que originen, en igualdad de condiciones, una discriminación arbitraria o injustificada contra terceros países o entre ellos, ni constituyan una restricción comercial encubierta

[40] WP12:Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 d la Directiva sobre protección de datos de la UE, aprobado por el Grupo de Trabajo el 24 de julio de 1998. Puede consultarse en http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_98.htm

[41] Dictamen 12/98, adoptado por el Grupo de Trabajo el 24 de julio de 1998: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos en la UE, aprobado por el Grupo de Trabajo el 24 de julio de 1998, (DG MARKT D/5025/98), que puede consultarse en Europa, sitio web de la Comisión Europea: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_98.htm.

	compromisos internacionales de la Comunidad.		contraria a los compromisos internacionales de la Comunidad.
		5	En el caso de Argentina, las normas de Derecho relativas a la protección de datos personales están reguladas mediante leyes generales y sectoriales, todas ellas de efecto jurídico obligatorio.
		6	Las normas generales están contempladas en la Constitución, la Ley 25 326 sobre protección de datos personales y el Decreto Reglamentario nº 1558/2001 (en lo sucesivo, «la legislación argentina»).
		7	La Constitución argentina prevé un recurso judicial especial, denominado *«habeas data*», para proteger los datos personales. Se trata de una subcategoría del procedimiento contemplado en la Constitución para proteger los derechos constitucionales y, por tanto, eleva la protección de datos personales a la categoría de derecho fundamental. De conformidad con el tercer párrafo del artículo 43 de la Constitución, toda persona podrá interponer esta acción (es decir, el *habeas data*) para tomar conocimiento de los datos que se refieren a ella y de su finalidad que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá vulnerarse el secreto de las fuentes de información periodística. La jurisprudencia argentina ha reconocido el *habeas data* como un derecho fundamental y directamente aplicable.
		8	La Ley 25 326 sobre protección de datos personales, de 4 de octubre de 2000 (en lo sucesivo denominada «la Ley») desarrolla y amplía lo dispuesto en la Constitución. Contiene normas sobre los principios generales de protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial *habeas dat*a.
		9	El Decreto Reglamentario nº 1558/2001, de 3 de diciembre de 2001 (en lo sucesivo denominado «el Reglamento») introduce las normas de aplicación de la Ley, completa lo dispuesto en ella y clarifica aspectos de la Ley que podrían interpretarse de manera divergente.

5	La Ley canadiense Personal Information and Electronic Documents Act (en adelante «la Ley canadiense») de 13 de abril de 2000 (3) se aplica a las entidades privadas que recojan, utilicen o divulguen datos personales en sus actividades comerciales. Entrará en vigor en tres etapas: A partir del 1 de enero de 2001, la Ley canadiense se aplicará a los datos personales, excluidos los de carácter sanitario, que las entidades que operen como «empresa federal» recojan, utilicen o divulguen en el transcurso de sus actividades económicas. Dichas empresas operan en sectores como el transporte aéreo, la banca, la radiotelevisión, el transporte interprovincial y las telecomunicaciones. También se aplicará a todos las entidades que comercian con datos personales fuera de su provincia o fuera del Canadá y a los datos laborales sobre los asalariados de las empresas federales. A partir del 1 de enero de 2002, se aplicará a los datos personales sanitarios de las entidades y actividades ya cubiertos en la primera etapa. A partir del 1 de enero de 2004, se ampliará a cualquier organismo que recoja, utilice o divulgue datos personales en el transcurso de una actividad comercial dentro de una provincia, independientemente de que dicho organismo esté o no regulado a escala federal. No están sujetas a la Ley canadiense las entidades a quienes se aplique la Federal Privacy Act o se regulen por el sector público de ámbito provincial. Del mismo modo, las actividades filantrópicas o sin fines lucrativos tampoco están sujetas a la Ley canadiense a no ser que tengan carácter comercial. No se aplica, por último, a los datos laborales utilizados con fines no comerciales siempre que no se refieran a los asalariados del sector privado sujeto a regulación federal. En tales casos, la autoridad canadiense de protección de la vida privada podrá proporcionar información adicional.	10	La legislación argentina cubre la protección de los datos personales contenidos en archivos, registros, bancos de datos u otros medios técnicos públicos y la protección de datos personales contenidos en archivos, registros, bancos de datos u otros medios técnicos privados «destinados a dar informes», incluidos «aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito».
		11	Determinadas normas de la Ley son aplicables de manera uniforme en todo el territorio argentino: disposiciones generales y disposiciones sobre los principios generales relativos a la protección de datos, derechos de los titulares de datos, obligaciones de los usuarios y responsables de archivos, registros y bancos de datos, sanciones penales, así como la existencia y características principales del recurso judicial *habeas data* tal como se establece en la Constitución.
		12	Otras disposiciones de la Ley son aplicables a los registros, archivos y bases o bancos de datos interconectados en red a nivel interjurisdiccional (es decir, interprovincial), nacional o internacional, y se considera que competen a la jurisdicción federal. Dichas disposiciones hacen referencia al control ejercido por el órgano de control, las sanciones impuestas por el órgano de control y el procedimiento aplicable en caso de recurso judicial *habeas data*. En cuanto a otros tipos de archivos, registros y bases de datos, debe considerarse que competen a la jurisdicción provincial y que las provincias pueden legislar al respecto.
		13	Asimismo, se incluyen normas sobre protección de datos en otros instrumentos jurídicos que regulan sectores diversos como, por ejemplo, las transacciones con tarjeta de crédito, las estadísticas, la banca o la salud.
6	A fin de que se respete el derecho de las provincias a legislar en su ámbito competencial, la Ley federal dispone que cuando éstas adopten una legislación básicamente similar, las entidades y ámbitos de organización y actividad que dicha legislación cubra estarán exentos de la Ley federal. El apartado 2 del artículo 26 de la Personal Information Protection and Electronic Documents Act faculta al Gobierno federal para, «si tiene el convencimiento de que una Ley provincial esencialmente similar a la presente parte se aplica a una organización —o categoría de entidades— o a una actividad —o categoría de actividades—, excluir la organización,		

	actividad o categoría de la aplicación de la presente parte en lo relativo a la recogida, utilización o comunicación de datos personales realizadas en el interior de la provincia». El Governor in Council (Gobierno federal canadiense) concede por decreto (Order-in-Council) las excepciones a la legislación que sea básicamente similar.		
7	Siempre que una provincia adopte una legislación básicamente similar, las entidades y ámbitos de organización y actividad que cubra estarán exentos de aplicar la Ley federal en transacciones en el interior de la provincia. La Ley federal seguirá aplicándose a toda recogida, utilización o divulgación de datos interprovincial internacional, así como en todos aquellos casos en que las provincias no hayan creado una legislación que sea básicamente similar ni total ni parcialmente.	15	El Gobierno argentino ha facilitado información y garantías sobre la manera en que debe interpretarse la legislación argentina, y ha garantizado que las normas argentinas en materia de protección de datos se aplican de conformidad con dicha interpretación. La presente Decisión se basa en las citadas informaciones y garantías y está subordinada a ellas, y, en particular, a las explicaciones y garantías proporcionadas por las autoridades argentinas sobre la manera en que debe interpretarse la legislación argentina en lo que se refiere a qué situaciones se hallan dentro del ámbito de aplicación de la legislación argentina de protección de datos.
		16	Por consiguiente, Argentina debería tener en cuenta la posibilidad de garantizar un nivel de protección adecuado para los datos personales según lo dispuesto en la Directiva 95/46/CE.
8	Canadá se adhirió formalmente el 29 de junio de 1984 a las Orientaciones de la OCDE sobre la protección de la vida privada y los flujos de datos transfronterizos de 1980. Canadá fue uno de los países que apoyó las Orientaciones de Naciones Unidas sobre los sistemas de información datos de carácter personal aprobadas por la Asamblea General el 14 de diciembre de 1990.		
9	La Ley canadiense comprende todos los principios fundamentales necesarios para que las personas físicas reciban una protección adecuada, pese a que también se dispongan excepciones y limitaciones para proteger importantes intereses públicos y dar reconocimiento a cierta información de dominio público. La aplicación de estas normas se garantiza mediante recursos jurisdiccionales y el control independiente que ejercen autoridades como el Comisario federal de protección de la vida privada, dotado de facultades de investigación intervención. Además, las disposiciones de Derecho canadiense relativas a la responsabilidad civil se aplican en caso de tratamiento ilícito que haya causado daños.	14	La legislación argentina comprende todos los principios fundamentales necesarios para que las personas físicas reciban una protección adecuada, pese a que también estén previstas excepciones y limitaciones para proteger intereses públicos importantes. La aplicación de estas normas está garantizada mediante un recurso judicial especial, simplificado y rápido, para proteger los datos personales, conocido como *«habeas data»*, junto con los recursos judiciales generales. La Ley prevé la creación de un órgano de control de protección de datos encargado de realizar todas las acciones necesarias para cumplir los objetivos y normas de la Ley y goza de atribuciones de investigación e intervención. En virtud del Reglamento, se creó la Dirección Nacional de Protección de Datos Personales como órgano de control. La legislación argentina prevé sanciones efectivas y disuasorias, tanto de naturaleza administrativa como penal. Además, en caso de que el tratamiento ilícito haya causado perjuicios, se aplican las normas de la

			legislación argentina relativas a la responsabilidad civil (tanto contractual como extracontractual).
10	Aunque se compruebe el nivel adecuado de la protección, por motivos de transparencia y para proteger la capacidad de las autoridades correspondientes de los Estados miembros de garantizar la protección de las personas en lo que respecta al tratamiento de sus datos personales, resulta necesario especificar en la presente Decisión las circunstancias excepcionales que pudieran justificar la suspensión de flujos específicos de información.	17	Aunque se haya comprobado el nivel adecuado de la protección, por motivos de transparencia y para proteger la capacidad de las autoridades correspondientes de los Estados miembros de garantizar la protección de las personas en lo que respecta al tratamiento de sus datos personales, resulta necesario especificar las circunstancias excepcionales que pueden justificar la suspensión de flujos específicos de información.
11	El Grupo de Trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, previsto en el artículo 29 de la Directiva 95/46/CE ha evacuado un dictamen sobre el nivel de protección que proporciona la Ley canadiense que se ha tenido en cuenta al preparar la presente Decisión[42].	18	El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la Directiva 95/46/CE, ha emitido un dictamen sobre el nivel de protección de los datos personales en Argentina, que ha sido tenido en cuenta al preparar la presente Decisión[43].
12	Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité previsto en el artículo 31 de la Directiva 95/46/CE.	19	Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité previsto en el apartado 1 del artículo 31 de la Directiva 95/46/CE.
ART	**REDACCIÓN**	**ART**	**REDACCIÓN**
1	A los efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, Canadá garantiza un nivel adecuado de protección de los datos personales transferidos desde la Comunidad a los receptores sujetos a la Personal Information Protection and Electronic Documents Act (en adelante «la Ley canadiense »).	1	A efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, se considera que Argentina garantiza un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad.
2	La presente Decisión se refiere únicamente a la adecuación de la protección que proporciona en Canadá la Ley canadiense, con arreglo a los requisitos del apartado 1 del artículo 25 de la Directiva 95/46/CE, y no afecta a otras condiciones o restricciones que se impusieren en aplicación de otros preceptos de la Directiva referentes al tratamiento de los datos personales en los Estados miembros.	2	La presente Decisión se refiere únicamente a la adecuación de la protección en Argentina con arreglo a los requisitos del apartado 1 del artículo 25 de la Directiva 95/46/CE y no afectará a otras condiciones o restricciones que puedan imponerse en aplicación de otras normas de la Directiva relativas al tratamiento de los datos personales en los Estados miembros.
3.1	Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con preceptos diferentes a los contemplados en el artículo 25 de la Directiva 95/46/CE, las autoridades de los Estados miembros podrán	3.1	Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las normas nacionales adoptadas de conformidad con preceptos diferentes a los contemplados en el artículo 25 de la Directiva 95/46/CE, las autoridades competentes de los Estados

[42] Dictamen 2/2001 sobre el nivel adecuado de protección de la ley canadiense Personal Information and Electronic Documents Act —WP 39 de 26 de enero de 2001. Puede consultarse en http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

[43] Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina — WP 63, de 3 de octubre de 2002, que puede consultarse en http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm.

	ejercer su facultad de suspender los flujos de datos hacia un receptor canadiense cuyas actividades entren en el ámbito de la Ley canadiense, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos en que: a) la autoridad competente canadiense compruebe que el receptor ha vulnerado las normas de protección aplicables, b) existan grandes probabilidades de que se estén vulnerando las normas de protección; existan razones para creer que la autoridad competente canadiense no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados; y las autoridades competentes del Estado miembro han hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad responsable del tratamiento en Canadá y proporcionarle la oportunidad de alegar. La suspensión cesará en cuanto esté garantizado el cumplimiento de las normas de protección y las autoridades correspondientes de la Comunidad hayan sido notificadas de ello.		miembros podrán ejercer su facultad de suspender los flujos de datos hacia un receptor argentino, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos en que: a) la autoridad competente argentina compruebe que el receptor ha vulnerado las normas de protección aplicables; o b) existan grandes probabilidades de que se estén vulnerando las normas de protección, existan razones para creer que la autoridad competente argentina no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia pueda crear un riesgo inminente de grave perjuicio a los afectados, y las autoridades competentes del Estado miembro hayan hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad responsable del tratamiento en Argentina y proporcionarle la oportunidad de alegar. La suspensión cesará en cuanto quede garantizado el cumplimiento de las normas de protección y las autoridades correspondientes de la Comunidad hayan sido notificadas de ello
3.2	Los Estados miembros informarán a la Comisión con la mayor brevedad de la adopción de medidas con arreglo al apartado 1.	3.2	Los Estados miembros informarán a la Comisión con la mayor brevedad de la adopción de medidas con arreglo al apartado 1.
3.3	Asimismo, los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en que la actuación de los organismos responsables del cumplimiento de las normas de protección en Canadá no garantice dicho cumplimiento.	3.3	Los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en que la actuación de los organismos responsables del cumplimiento de las normas de protección en Argentina no garantice dicho cumplimiento.
3.4	Si la información recogida con arreglo a los apartados 1 a 3 demuestra que los organismos responsables del cumplimiento de las normas de protección en Canadá no están ejerciendo su función, la Comisión lo notificará a la autoridad competente canadiense y, si procede, presentará un proyecto de medidas con arreglo al procedimiento que contempla el apartado 2 del artículo 31 de la Directiva 95/46/CE, a fin de anular o suspender la presente Decisión o limitar su ámbito de aplicación.	3.4	Si la información recogida con arreglo a los apartados 1 a 3 demuestra que los organismos responsables del cumplimiento de las normas de protección en Argentina no están ejerciendo su función, la Comisión lo notificará a la autoridad competente argentina y, si procede, presentará un proyecto de medidas con arreglo al procedimiento contemplado en el apartado 2 del artículo 31 de la Directiva 95/46/CE, a fin de anular o suspender la presente Decisión o limitar su ámbito de aplicación.
4.1	La presente Decisión podrá adaptarse en cualquier momento de conformidad con la experiencia de su funcionamiento o los cambios que se introduzcan en la legislación canadiense, señaladamente en las medidas por las que se reconoce que una provincia canadiense tiene una legislación substancialmente similar. La Comisión analizará, basándose en la información disponible, la aplicación de la presente Decisión tres años después de su notificación a los Estados miembros. Informará al Comité	4.1	La presente Decisión podrá adaptarse en cualquier momento de conformidad con la experiencia de su funcionamiento o los cambios de la legislación argentina, su aplicación o su interpretación. La Comisión supervisará el funcionamiento de la presente Decisión e informará al Comité previsto en el artículo 31 de la Directiva 95/46/CE de cualquier hecho pertinente y, en particular, de cualquier prueba que pueda afectar a la resolución del artículo 1 de la presente Decisión, relativa a que la

	contemplado en el artículo 31 de la Directiva 95/46/CE de cualquier hecho que venga al caso, en particular de cualquier prueba que pueda afectar a la resolución contenida en el artículo 1 de la presente Decisión de que la protección en Canadá es adecuada a efectos del artículo 25 de la Directiva 95/46/CE, así como de cualquier prueba de que la presente Decisión se está aplicando de forma discriminatoria.		protección en Argentina es adecuada a efectos del artículo 25 de la Directiva 95/46/CE, así como de cualquier prueba de que la presente Decisión se está aplicando de forma discriminatoria.
4.2	La Comisión presentará, si procede, proyectos de medidas de conformidad con el procedimiento establecido en el apartado 2 del artículo 31 de la Directiva 95/46/CE.	4.2	La Comisión presentará, si es necesario, proyectos de medidas de conformidad con el procedimiento establecido en el apartado 2 del artículo 31 de la Directiva 95/46/CE.
5	Los Estados miembros adoptarán todas las medidas necesarias para cumplir la presente Decisión, a más tardar en un plazo de noventa días a partir de la fecha de su notificación a los Estados miembros.	5	Los Estados miembros adoptarán todas las medidas necesarias para cumplir la presente Decisión, a más tardar en un plazo de ciento veinte días a partir de la fecha de su notificación a los Estados miembros.
6	Los destinatarios de la presente Decisión serán los Estados miembros.	6	Los destinatarios de la presente Decisión serán los Estados miembros.

En resumen, los principios que rigen la TID a nivel comunitario son:

- ❒ Prohibición de transferencias a un país tercero que no garantice un nivel de protección adecuado (art. 25.1 Directiva 95/46/CE).
- ❒ La Comisión podrá adoptar una Decisión en la que establezca que un país tercero garantiza un nivel de protección adecuado, en cuyo caso los Estados miembros tendrán que adoptar las medidas necesarias para adecuarse a la misma (art. 25.6 Directiva 95/46/CE).

A.2) Excepciones:

Las excepciones a estos principios se encuentran tasadas en el artículo 26 que dispone

"1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o
b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o
c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos

derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.
Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión[44]*."*

La utilización de las cláusulas contractuales tipo a las que hace referencia este último apartado del artículo 26 de la Directiva 95/46/CE se prevé como una solución específica a la necesidad de garantizar el cumplimiento de las disposiciones en materia de protección de datos en el caso de aquellas transferencias de datos que se efectúan con destino a países que no proporcionan un nivel adecuado de protección.

Las cláusulas contractuales tipo, que han sido aprobadas mediante las correspondientes Decisiones de la Comisión, en función de cuál sea la finalidad de la transferencia, se refieren únicamente a la protección de datos, pudiendo añadirse por las partes del contrato aquellas otras cláusulas que sean necesarias para el desarrollo de su negocio.

El uso de las cláusulas contractuales está destinado a aquellos supuestos en que se vayan a transferir datos a un tercer país que no proporcione un nivel adecuado, pudiendo distinguir dos tipos de cláusulas en función de cuál sea la finalidad de la transferencia:

[44] Decisiones de la Comisión por las que se aprueban cláusulas contractuales tipo para la transferencia internacional de datos:

- Decisión 2001/497/CE de la Comisión, de 15 de junio, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país prevista en la Directiva 95/46/CE.
- Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE.

- ❒ entre un responsable del tratamiento (establecido en el territorio de la Unión Europea) y un responsable del tratamiento (establecido en un tercer país), y
- ❒ entre un responsable del tratamiento (establecido en el territorio de la Unión Europea) y un encargado del tratamiento (establecido en un tercer país).

En estos contratos las partes contratantes son el exportador de datos, establecido en el territorio de algún Estado miembro de la Unión Europea (UE), y el importador de datos, que podrá ser un responsable del tratamiento o un encargado del tratamiento, establecido en un país tercero, fuera del territorio de la UE. Por su parte, los interesados, titulares de los datos que son objeto de tratamiento no son parte del contrato, si bien en las cláusulas contractuales tipo de las que se haga uso deberá preverse la protección de los mismos como beneficiarios.

Los principios y condiciones que deben concurrir en el contrato, y que resultan básicos para la protección de datos, en aras a garantizar al interesado cuyos datos son objeto de tratamiento y transferencia una protección adecuada, son:

- ❒ principio de limitación de objetivos;
- ❒ principio de proporcionalidad y calidad de datos;
- ❒ principio de transparencia;
- ❒ principio de seguridad;
- ❒ derecho de acceso, rectificación y oposición;
- ❒ restricciones respecto a transferencias sucesivas a personas ajenas al contrato.

A los anteriores principios deben sumarse otros que resultan complementarios (relativos a los datos especialmente protegidos, mercadotecnia directa y decisiones automatizadas).

La evaluación de la efectividad de una solución contractual en la transferencia de datos a un tercer país vendrá por la aplicación de los mismos criterios que se exigen para un sistema de protección de datos, es decir:

- ❒ ofrecer un nivel satisfactorio de cumplimiento de las normas,
- ❒ facilitar apoyo y asistencia a los interesados en el ejercicio de sus derechos, y
- ❒ proporcionar vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

Por último, cabe señalar que una de las dificultades que plantea el enfoque contractual es la posibilidad de que las normas jurídicas generales del tercer país de que se trate obliguen al receptor de la transferencia, en determinadas circunstancias, a comunicar los datos personales a las autoridades y de que tales requisitos prevalezcan sobre todo contrato firmado por el encargado del tratamiento.

A.3) Conclusiones:

Vistos los principios y las excepciones, resumimos que podrá llevarse a cabo una transferencia de datos a un país tercero en los siguientes supuestos:

1. Cuando se declare el nivel de protección adecuado en el tercer país receptor de los datos.
2. Cuando se esté en una de las excepciones tasadas en la Directiva.
3. Cuando se haga uso de un mecanismo contractual que cumpla las garantías de la protección de datos aunque el país receptor no garantice un nivel de protección adecuado.

En conclusión, las transferencias de datos un país tercero podrán llevarse a cabo cuando:

- ❒ el país tercero destinatario de los datos esté declarado como país que proporciona un nivel adecuado de protección, o
- ❒ el país de destino no proporcione un nivel adecuado de protección y no estemos en una de las excepciones del artículo 26 de la Directiva 95/46/CE, pero se opte por el modelo de contrato propuesto por la Comisión, cuyas cláusulas ofrecerán las garantías respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas y el respeto al ejercicio de los respectivos derechos.

A.4) Análisis del Acuerdo de Puerto Seguro:

El Acuerdo de "Puerto Seguro" es fruto de la negociación mantenida, durante más de dos años, entre el Departamento de Comercio de Estados Unidos (EE.UU.) y la Comisión Europea, partiendo de los diferentes enfoques que los EE.UU. y la UE dan a la protección de la vida privada de sus ciudadanos, basándose el planteamiento de los EE.UU. en una mezcla de normas legales y autorregulación por parte del sector privado.

Vamos a pasar a analizar brevemente esta Decisión por sus peculiaridades, ya que es una Decisión que, contrariamente a las demás, NO declara un nivel adecuado en el país de destino, esto es, EE.UU., sino que establece que las empresas de ese país que se adhieran a este sistema de garantías, podrán ser consideradas como un destino adecuado de los datos transmitidos desde la Unión Europea.

1) Decisión de la Comisión Europea:

Estas negociaciones dieron lugar a la aprobación por la Comisión Europea de la Decisión 2000/520/CE de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo Europeo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas mas frecuentes publicadas por el Departamento de Comercio de los Estados Unidos de América.

Mediante la aplicación de dicho Acuerdo, las entidades estadounidenses, que voluntariamente decidan adherirse a los principios contenidos en el mismo, podrán recibir datos personales de responsables establecidos en alguno de los Estados miembros de la UE al entenderse que dichas entidades proporcionan una protección suficiente.

2) Principios del Acuerdo de Puerto Seguro:

Los Principios que conforman el puerto seguro se concretan en los de:

- **Notificación:** significa que las entidades informarán a los interesados de cuál es la finalidad con la que se recogen sus datos; la forma de contactar con ellas para cualquier pregunta o queja; los tipos de terceros a los cuales se revelará la información; las opciones y medios que la entidad ofrece a los particulares para limitar su uso y su divulgación.
- **Opción:** los interesados tendrán la posibilidad de decidir (exclusión) si su información personal: a) puede divulgarse a un tercero, o b) puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida o no haya sido autorizado posteriormente por el particular.
- **Transferencia ulterior:** supone que para revelar información a terceros, las entidades deberán aplicar los principios de notificación y opción.

- ❒ **Seguridad:** las entidades adoptarán las medidas razonables para evitar su pérdida, su mal uso y consulta no autorizada, su divulgación, su modificación y su destrucción.
- ❒ **Integridad de los datos:** los datos tendrán que ser pertinentes para los fines con los que se utilizan, y también tendrán que ser exactos, completos y actuales. Una entidad no podrá tratar la información personal de manera incompatible con los fines que motivaron su recogida o aprobó posteriormente el particular.
- ❒ **Acceso:** los interesados deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si resultase inexacta, excepto en dos casos: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la vida privada de la persona; o cuando puedan vulnerarse los derechos de otras personas.
- ❒ **Aplicación:** significa que con el fin de garantizar una protección eficaz de la vida privada deben preverse mecanismos para cumplir con los principios, una vía de recurso para las personas a que se refieran los datos y se vean afectadas por el incumplimiento de dichos principios y sanciones contra la entidad incumplidora. Además establece los requisitos que, como mínimo, deben cumplir dichos mecanismos.

3) Aplicación de los principios:

La aplicación de los principios del Puerto Seguro se llevará a cabo según unas pautas de actuación que son las que proporcionan las Preguntas Más Frecuentes[45] (FAQ) que fueron publicadas en su momento, y como Anexo de la

[45] Las Preguntas Más Frecuentes (FAQ) incluidas en el Anexo II de la Decisión 2000/520/CE se refieren a:

FAQ 1.- Datos especialmente protegidos
FAQ 2.- Excepciones del periodismo
FAQ 3.- Responsabilidad subsidiaria
FAQ 4.- Bancos de inversiones y sociedades de auditoría
FAQ 5.- La función de las autoridades de protección de datos
FAQ 6.- Autocertificación
FAQ 7.- Verificación
FAQ 8.- Acceso
FAQ 9.- Recursos humanos
FAQ 10.- Contratos del artículo 17
FAQ 11.- Resolución de litigios y ejecución
FAQ 12.- Opción – Momento de la exclusión
FAQ 13.- Información sobre viajes
FAQ 14.- Productos médicos y farmacéuticos
FAQ 15.- Información extraída de registros públicos e información de dominio público

Decisión adoptada por la Comisión Europea, por el Departamento de Comercio de los EE.UU. respecto de aquellas cuestiones que pudieran suscitar alguna duda o que requieren explicación.

A efectos de cumplir con lo establecido en los principios y en las FAQ, las entidades que decidan adherirse al Acuerdo podrán seguir alguna de las siguientes opciones:

a) por adhesión a un programa de autorregulación que ya los contenga, o
b) por autorregulación de la entidad en cuestión si dicha autorregulación los respeta.

En cualquier caso, es necesario que el código de autorregulación aplicado por la entidad en cuestión "se adecue a dichos principios".

4) Adhesión de las entidades norteamericanas:

Los beneficios del puerto seguro se obtienen desde la fecha en que una entidad se adhiere a este sistema mediante autocertificación, que puede ser una carta firmada por uno de los responsables de la entidad, ante el Departamento de Comercio, y aplicándose sobre todos los datos personales recibidos desde la UE.

La adhesión por parte de las entidades al puerto seguro es totalmente voluntaria, produciéndose mediante autocertificación dirigida al Departamento de Comercio, lo que significa que son las propias entidades las que manifiestan que cumplen con los principios y las correspondientes FAQ.

El Departamento de Comercio mantendrá una lista de las entidades que presenten las cartas de autocertificación, haciendo públicas tanto aquéllas como éstas (disponible en www.export.gov/safeharbor), indicándolo también en sus respectivas políticas de protección de la vida privada. Dicha lista será actualizada con las cartas que, al menos una vez al año deberán presentarse por las entidades que quieran beneficiarse del puerto seguro. La falta de presentación de la carta determina la exclusión de los beneficios otorgados.

Es necesario que se sometan a uno de los organismos jurídicos reconocidos en el Anexo, que son:

- la FTC *(Federal Trade Commission),*o
- el Departamento de Transporte (DoT)

para que dichos organismos tengan competencia y "jurisdicción" sobre sus actuaciones.

B) Legislaciones de protección de datos de Argentina, Canadá y España:

Al igual que en el análisis de la Directiva, vamos a diferenciar entre la regla general y las excepciones a la misma en materia de TID.

B.1) Regla general:

LOPD	LEY Nº 25326.	PIPED Act
Transferencia Internacional de Datos		
Art. 33	**Art. 12.1**	
1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas. 2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.	Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.	

B.2) Excepciones:

LOPD	LEY Nº 25326.	PIPEDAct
Transferencia Internacional de Datos		
Art. 34	**Art. 12.2**	
a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.	d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;	
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.	a)Colaboración judicial internacional;	
c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.	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;	
d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.	c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;	
	Art. 12 del Reglamento	
e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.	La prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión.	
f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado. g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.		
h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus		

competencias. i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.		
	Art. 12 del Reglamento	
j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.	No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta.	
	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."	
	Art. 12 del Reglamento	
k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.	Facúltase a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional. Si llegara a la conclusión de que un Estado u organismo no protege adecuadamente a los datos personales, elevará al PODER EJECUTIVO NACIONAL un proyecto de decreto para emitir tal declaración. El proyecto deberá ser refrendado por los Ministros de Justicia y Derechos Humanos y de Relaciones Exteriores, Comercio Internacional y Culto. El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de	

	destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares o que resulten aplicables a los organismos internacionales o supranacionales. Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación., o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales.	

Del análisis de las legislaciones contenidas en la tabla anterior deducimos, sin perjuicio de las muchas excepciones que se recogen en ambas legislaciones, que los países destinatarios de las TID deben reunir un nivel adecuado de protección para que la TID no requiera otro requisito y así este nivel adecuado de protección se examinará atendiendo a distintos requisitos.

Para la LOPD, será la Agencia Española de Protección de Datos la que realizará la evaluación de si un país proporciona o no un nivel adecuado de protección a los datos de carácter personal, atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos.

En particular, se tendrán en consideración las siguientes circunstancias:

- la naturaleza de los datos,
- la finalidad y la duración del tratamiento o de los tratamientos previstos,
- el país de origen y el país de destino final,
- las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate,
- el contenido de los informes de la Comisión de la Unión Europea,
- así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Además, es necesario tener en consideración la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos, y que permite conocer

cuál es el criterio seguido por el órgano de vigilar el cumplimiento de la normativa en protección de datos cuando se trata de una transferencia internacional de datos. Dicha Instrucción, aplicable a todos los supuestos de transferencia internacional de datos, se divide en dos secciones. La Sección primera contiene disposiciones generales aplicables a todos los supuestos de TID, incluyendo en primer lugar la definición de transferencia y recordando que en todo caso tiene que cumplirse con las disposiciones de la LOPD para poder llevar a cabo una transferencia. A continuación, recuerda la obligación del responsable del tratamiento de comunicar al Registro General de Protección de Datos las transferencias que se efectúen para que así conste en la inscripción del sistema de datos correspondiente. Por su parte, la Sección segunda atiende a los diferentes supuestos estableciendo normas aplicables en función: a) del país de destino, en virtud de que se trate de un tercer país con un nivel adecuado o no, y b) de la finalidad de la transferencia, pudiendo ser ésta una cesión de datos (entre responsables de sistemas de datos personales) o una prestación de servicios (entre un responsable del sistema de datos personales y un encargado del tratamiento).

En la normativa argentina sobre protección de datos se establecen como criterios para determinar un nivel adecuado de protección los siguientes:

1.- El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos;

2.- En particular:

- la naturaleza de los datos,
- la finalidad y la duración de tratamiento o de los tratamientos previstos,
- el lugar de destino final,
- las normas de derecho, generales o sectoriales, vigentes en el país de que se trate,
- así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares o que resulten aplicables a los organismos internacionales o supranacionales.

3.- Por último, se dispone que se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente:

- del ordenamiento jurídico vigente,
- de sistemas de autorregulación.,
- del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales.

Por su parte la normativa mexicana sobre la materia realiza la siguiente referencia:

> Lineamiento 24: *En caso de que el o los destinatarios de los datos sean personas o instituciones de otros países, las dependencias y entidades deberán asegurarse que tales países garanticen que cuentan con niveles de protección semejantes o superiores a los establecidos en estos Lineamientos, y en la normatividad propia de la dependencia o entidad de que se trate.*

Siendo esta la única referencia que encontramos en el texto normativo de los Lineamientos en materia de protección de datos, recomendamos considerar, que si bien debe buscarse ese nivel adecuado de protección en los países destinatarios de la TID, sería conveniente regular otras cuestiones que hacen referencia a:

- la autoridad que va a ser competente para determinar dicho nivel adecuado,
- los criterios conforme a los cuales va a considerarse ese nivel adecuado de protección,
- las excepciones en las que a pesar de no evaluarse el nivel adecuado de protección del país destinatario de la TID va a procederse a realiza r la transferencia de datos, por ejemplo, en los casos en los que el titular de los datos consienta la transferencia, dado que siendo el principio de consentimiento uno de los principios básicos en materia de protección de datos, el titular de los datos puede de este modo autorizar la transferencia.

Conclusiones: la Transferencia Internacional de Datos (TID) supone que los datos salgan fuera de las fronteras del territorio nacional, de manera que hay al menos dos ordenamientos jurídicos que entran en juego, siendo necesario garantizar en cualquier caso el nivel de protección de datos que el ordenamiento jurídico proporcione a los interesados en su país de origen. En este sentido, en la TID tiene que buscarse que el país de destino de la transferencia proporcione un nivel adecuado de protección de datos con el propósito de garantizar el derecho a la protección de datos de los interesados.

En la TID, y del análisis de las diferentes normas sobre protección de datos, se sigue la regla general de prohibición de transferencias a terceros países que no proporcionen un nivel adecuado, y ello con el propósito de garantizar la protección debida a los interesados.

A efectos de su análisis, la TID puede clasificarse atendiendo a dos criterios: el país de destino y la finalidad de la transferencia. Así, en el primer caso puede distinguirse entre países que tengan un nivel adecuado, países a los que se haya reconocido un nivel adecuado y países que no proporcionen un nivel adecuado. Y en el segundo caso, la TID puede tener como finalidad una cesión o comunicación de datos o una prestación de servicios por parte de un encargado del tratamiento.

En cualquier caso, la realización de una TID requiere que el tratamiento de datos personales que supone cumpla con todos los requisitos de la normativa que regula la protección de datos en el país de origen, siendo aquí necesario considerar aspectos tales como la potestad del órgano de control para declarar que un tercer país proporciona un nivel adecuado o, en su caso, comprobar el efectivo cumplimiento de las obligaciones por parte del destinatario de la cesión.

Además de lo anterior, en toda TID se busca que la protección conferida a los interesados quede garantizada, siendo obligación del responsable del tratamiento que va a efectuar dicha transferencia aportar garantías suficientes para que el órgano de control, si ello fuese necesario, otorgue su autorización a la realización de la transferencia. Por último, es necesario tener en consideración la inclusión de excepciones, tasadas en la Ley.

6. CÓDIGOS DE CONDUCTA

Los códigos tipo, códigos de conducta, éticos o deontológicos en el ámbito europeo y en el anglosajón son instrumentos de autorregulación, especialmente aptos para adaptar los diversos preceptos de una ley a las características específicas de cada sector, y, en la materia objeto de nuestro estudio en concreto, lo que se pretende conseguir con estos códigos es que todo aquel que intervenga en el tratamiento de datos asimile y se conciencie de la importancia de la protección de los datos de carácter personal.

Estos códigos tipo son voluntarios, en el sentido de que las partes deciden libremente su adhesión a los mismos, y no tienen carácter de norma jurídica en el sentido de emanar del Poder Legislativo del Estado, sin embargo, como su contenido ha de respetar plenamente los principios y derechos reconocidos a las personas en la normativa sobre protección de datos es conveniente cumplir lo dispuesto en ellos ya que, de otro modo, se estaría vulnerando lo previsto en dicha normativa. Además, la efectividad del código vendrá dada por la aplicación de las sanciones que se prevean en el mismo y la autoridad de quien las imponga.

Estos códigos también pueden tener el carácter de códigos deontológicos o de buena práctica profesional y pueden constituir un medio a través del cual el titular del sistema de datos personales pueda ofrecer a los ciudadanos de una garantía de conocimiento y cumplimiento de la normativa sobre protección de datos. De este modo, es posible que los interesados accedan a su contenido con el objeto de conocer el sistema de recogida, tratamiento y uso de los datos de carácter personal, a través de copias de los códigos tipo que se depositen o inscriban en un órgano dependiente de la autoridad de control o en la propia autoridad de control.

El acceso al contenido de los códigos de conducta puede proporcionarse electrónicamente y, con la finalidad de darles mayor difusión, podría fomentarse su traducción a otros idiomas.

En el ámbito nacional es importante que se encargue a determinados organismos el impulso para la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores. En este sentido, puede establecerse la participación de las asociaciones y organizaciones

representativas en la elaboración de estos códigos y la creación de un distintivo que permita identificar a quienes respeten los códigos de conducta que se adopten.

En relación con los códigos tipo, de conducta o deontológicos el Convenio 108 no establece regulación alguna a lo largo de su articulado. En este sentido, el artículo 27 de la Directiva 95/46/CE dispone:

> *"1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.*
>
> *2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales.*
>
> *Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.*
>
> *3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo."*

En las normas que venimos estudiando también se encuentran referencias a la materia:

LOPD	LEY Nº 25326	PIPED Act
CÓDIGOS DE CONDUCTA		
Art. 32[46]	**Art. 30**	**Division 3**
1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo. 2. Los citados códigos podrán	1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que 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. 2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia. **Art. 30 Decreto**	24. The Commissioner shall (a) develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part; (b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry; (c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10; and (d) promote, by any means that the Commissioner considers

[46] El R.D. 1332/94 dispone respecto de los Códigos Tipo en el artículo 9 relativo a la Inscripción y publicidad de los códigos tipo que:
"1. Los códigos tipo se depositarán, para su inscripción, en el Registro General de Protección de Datos.
2. El Director de la Agencia de Protección de Datos podrá denegar la inscripción si el código tipo no se ajusta a las disposiciones de la Ley Orgánica 5/1992 y del presente Real Decreto, sin perjuicio de requerir a los solicitantes para que subsanen las deficiencias.
3. Los particulares podrán obtener copias de los códigos tipo depositados e inscritos en el Registro General de Protección de Datos.
4. En caso de incumplimiento de las normas contenidas en los códigos tipo se estará a lo dispuesto al efecto en los acuerdos o decisiones que los formulen."

contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél. 3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia Española de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.	La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES alentará la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por la Ley Nº 25.326 y esta reglamentación. Las asociaciones de profesionales y las demás organizaciones representantes de otras categorías de responsables o usuarios de archivos, registros, bases o bancos de datos públicos o privados, que hayan elaborado proyectos de códigos éticos, o que tengan la intención de modificar o prorrogar códigos nacionales existentes, podrán someterlos a consideración de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, la cual aprobará el ordenamiento o sugerirá las correcciones que se estimen necesarias para su aprobación.	appropriate, the purposes of this Part.

Tal y como se desprende de la tabla anterior, y teniendo en cuenta que la legislación mexicana no regula los códigos tipo y que la norma canadiense solamente hace una somera referencia a los mismos, las legislaciones española y argentina son las que con más detalle regulan esta materia.

Conclusiones: tras el análisis de las normas que a nivel internacional regulan la protección de datos, resulta conveniente que en el articulado de una norma sobre protección de datos, y con el propósito de garantizar a los interesados un elevado nivel de protección de datos, se incluya una referencia a la posibilidad de que, tanto por parte del sector público como del sector privado, los responsables de sistemas de datos de carácter personal o las organizaciones en las que se integren, puedan desarrollar códigos (éticos, tipo, deontológicos, de conducta o de buena práctica) para adecuar determinados aspectos de su aplicación práctica a las particularidades de un sector.

Si bien estos códigos cumplen una función distinta en el ordenamiento jurídico anglosajón y en el europeo, deben proporcionar en todo caso un elevado grado

de protección a los interesados, garantizándose su cumplimiento a través de sanciones que tendrán que ser respaldadas por un órgano que tenga poder suficiente para imponerlas y hacerlas cumplir, dependiendo la efectividad del código en gran medida de esto último.

7. ÓRGANO DE CONTROL

El órgano de control, en el ejercicio de las funciones que se le atribuyan, ha de velar por el cumplimiento de la normativa sobre protección de datos, para lo cual puede ejercer las potestades inspectora, sancionadora y cualesquiera otras que se le asignen. Asimismo, y si fuera necesario, puede requerir la adopción de las medidas necesarias para adecuar el tratamiento de datos a las disposiciones de las normas.

Además, puede dar publicidad de los sistemas de datos de carácter personal que hayan sido inscritos o notificados a través del órgano correspondiente, pudiendo constatarse aquí la existencia de un Registro en algunas de las normas internacionales que venimos analizando.

Entre las funciones que pueden atribuirse al órgano de control se pueden destacar:

a) Garantizar el cumplimiento de la legislación sobre protección de datos;
b) Requerir a los responsables de los tratamientos la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones vigentes;
c) Ejercer las potestades inspectora, sancionadora y cualesquiera otras en los términos previstos;
d) Garantizar la publicidad de los sistemas de datos de carácter personal que le sean notificados a través del órgano correspondiente;

En el establecimiento de un órgano de control para el desempeño de determinadas funciones en materia de protección de datos hay que tener en cuenta qué competencias le van a ser atribuidas, cómo se deben ejercer las funciones a desempeñar y cuáles serán las asignaciones económicas que le correspondan.

Respecto de este apartado del informe hay que tener en cuenta que el Convenio 108 no contempla en su articulado a los órganos o autoridades de control.

7.1. Régimen y competencias

En la Directiva 95/46/CE:

En relación con las autoridades de control, el artículo 28 de la Directiva 95/46/CE dispone:

> *"1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.*
>
> *Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.*
>
> *2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.*
>
> *[...]*
>
> *6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro. [...]"*

En las normas nacionales:

LOPD	LEY Nº 25326	PIPED Act
ÓRGANO DE CONTROL		
Art. 35	**Art. 29.1 Decreto**	
1. La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el	Créase la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, en el ámbito de la SECRETARIA DE JUSTICIA Y ASUNTOS LEGISLATIVOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, como órgano de control de la Ley Nº 25.326.	
	Art. 29	

Gobierno. 2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia Española de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.	1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. 2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.	
3. Los puestos de trabajo de los órganos y servicios que integren la Agencia Española de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.		
	Art. 29.3 Decreto	
4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos: a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado. b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo. c) Cualesquiera otros que legalmente puedan serle atribuidos.	La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES se financiará a través de: a) lo que recaude en concepto de tasas por los servicios que preste; b) el producido de las multas previstas en el artículo 31 de la Ley Nº 25.326; c) las asignaciones presupuestarias que se incluyan en la Ley de Presupuesto de la Administración Nacional a partir del año 2002.	
5. La Agencia Española de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.		

Las normas objeto del presente análisis han previsto un órgano de control; en España se denomina “Agencia Española de Protección de Datos”, en Argentina es la “Dirección Nacional de Protección de Datos Personales” y en México el

"Instituto Federal de Acceso a la Información Pública", si bien en este último caso es necesario tener en consideración que no puede considerarse una Agencia de Protección de Datos como tal al no tener todas las funciones de aquélla tal y como vemos al analizar las normas sobre protección de datos. La norma canadiense no establece expresamente un precepto por el que se cree su órgano de control pero, a lo largo de su articulado, hacer referencia a un órgano que denomina *"Commissioner"*.

El *Privacy Commsioner* canadiense se define como un *"ombudsman"*, en clara referencia a la figura de defensor del pueblo de gran tradición europea e internacional, por lo que su labor se centra en intentar resolver los conflictos en primera instancia mediante la mediación y la conciliación. En este sentido, el Comisionado canadiense informa directamente al Parlamento, y tiene además dos ayudantes comisionados y un comité externo, recientemente creado en febrero de 2004. Entre sus competencias se incluyen las de investigar las quejas y conducir las reclamaciones, que los individuos le pueden plantear de acuerdo a lo previsto en el artículo 29 y 11 de su ley referentes al sector público y privado respectivamente, publicar información sobre las prácticas en el manejo de la información personal en los sectores público y privado, conducir investigaciones sobre temas de interés, y promover el respeto y entendimiento de los temas sobre la privacidad.

En el caso de México hay que estar a lo dispuesto por el artículo 33 de la LAI que establece:

> *"El Instituto Federal de Acceso a la Información Pública es un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho de acceso a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades."*

Cada una de las normas analizadas someten al órgano de control a un régimen jurídico y composición distintos como consecuencia de la diferencia de regímenes normativos que están vigentes en cada país.

7.2. Funciones

En la Directiva 95/46/CE:

La Directiva 95/46/CE regula las funciones de los órganos de control estableciendo en el apartado 2 de su artículo 21 la obligación de que:

"Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18."

Asimismo, a lo largo del artículo 28 de la Directiva 95/46/CE se encuentran las funciones correspondientes a los órganos de control de los Estados miembros. En concreto, se prevén las siguientes:

"3. La autoridad de control dispondrá, en particular, de:

- *poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;*
- *poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;*
- *capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.*

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.

5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.

6. [...]

Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.

7. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso."

En las normas nacionales:

LOPD	LEY Nº 25326	PIPED Act
ÓRGANO DE CONTROL		
Art. 37	**Art. 29.1**	**Division 3**
Son funciones de la Agencia Española de Protección de Datos: a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias. c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley. d) Atender las peticiones y reclamaciones formuladas por las personas afectadas. e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal. f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones. g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley. h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley. i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones. j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente	A tales efectos tendrá las siguientes funciones y atribuciones: a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza; b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley; c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos; d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley; e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados; f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia; g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley; h) Controlar el cumplimiento de	19. (1) After an audit, the Commissioner shall provide the audited organization with a report that contains the findings of the audit and any recommendations that the Commissioner considers appropriate. 2) The report may be included in a report made under section 25. 20. (1) Subject to subsections (2) to (5), 13(3) and 19(1), the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part. (2) The Commissioner may make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so. (3) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information that in the Commissioner's opinion is necessary to (a) conduct an investigation or audit under this Part; or (b) establish the grounds for findings and recommendations contained in any report under this Part. (4) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information in the course of (a) a prosecution for an offence under section 28; (b) a prosecution for an offence under section 132 of the Criminal Code (perjury) in respect of a statement made

una relación de dichos ficheros con la información adicional que el Director de la Agencia determine. k) Redactar una memoria anual y remitirla al Ministerio de Justicia. l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales. m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46. n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.	los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.	under this Part; (c) a hearing before the Court under this Part; or (d) an appeal from a decision of the Court. (5) The Commissioner may disclose to the Attorney General of Canada or of a province, as the case may be, information relating to the commission of an offence against any law of Canada or a province on the part of an officer or employee of an organization if, in the Commissioner's opinion, there is evidence of an offence. 21. The Commissioner or person acting on behalf or under the direction of the Commissioner is not a competent witness in respect of any matter that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part in any proceeding other than (a) a prosecution for an offence under section 28; (b) a prosecution for an offence under section 132 of the Criminal Code (perjury) in respect of a statement made under this Part; (c) a hearing before the Court under this Part; or (d) an appeal from a decision of the Court. 22. (1) No criminal or civil proceedings lie against the Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported or said in good faith as a result of the performance or exercise or purported performance or exercise of any duty or power of the Commissioner under this Part. (2) For the purposes of any law relating to libel or slander, (a) anything said, any information supplied or any record or thing produced in good faith in the course of an investigation or audit carried out by or on behalf of the Commissioner under this Part is privileged; and

		(b) any report made in good faith by the Commissioner under this Part and any fair and accurate account of the report made in good faith for the purpose of news reporting is privileged.
		23. (1) If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under provincial legislation that is substantially similar to this Part, has powers and duties similar to those of the Commissioner. (2) The Commissioner may enter into agreements with any person with whom the Commissioner may consult under subsection (1) (a) to coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested; (b) to undertake and publish research related to the protection of personal information; and (c) to develop model contracts for the protection of personal information that is collected, used or disclosed interprovincially or internationally.

		24. The Commissioner shall (a) develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part; (b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry; (c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10; and (d) promote, by any means that the Commissioner considers appropriate, the purposes of this Part.
		25. (1) The Commissioner shall, as soon as practicable after the end of each calendar year, submit to Parliament a report concerning the application of this Part, the extent to which the provinces have enacted legislation that is substantially similar to this Part and the application of any such legislation. (2) Before preparing the report, the Commissioner shall consult with those persons in the provinces who, in the Commissioner's opinion, are in a position to assist the Commissioner in reporting respecting personal information that is collected, used or disclosed interprovincially or internationally.
		27. (1) Any person who has reasonable grounds to believe that a person has contravened or intends to contravene a provision of Division 1, may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification. (2) The Commissioner shall keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

		27.1 (1) No employer shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment, by reason that (a) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene a provision of Division 1; (b) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of a provision of Division 1; (c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order that a provision of Division 1 not be contravened; or (d) the employer believes that the employee will do anything referred to in paragraph (a), (b) or (c). (2) Nothing in this section impairs any right of an employee either at law or under an employment contract or collective agreement. (3) In this section, "employee" includes an independent contractor and "employer"' has a corresponding meaning.
Art. 40		**Divison 3**
Potestad de inspección. 1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados. 2. Los funcionarios que ejerzan la		18. (1) The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening a provision of Division 1 or is not following a recommendation set out in Schedule 1, and for that purpose may (a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary for the audit,

inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos. Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.		in the same manner and to the same extent as a superior court of record; (b) administer oaths; (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law; **(d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by the organization on satisfying any security requirements of the organization relating to the premises;** (e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and (f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the audit. (2) The Commissioner may delegate any of the powers set out in subsection (1). (3) The Commissioner or the delegate shall return to a person or an organization any record or thing they produced under this section within ten days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced. (4) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(d).
Art. 49		
Potestad de inmovilización de ficheros En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que		

se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia Española de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.		

En relación con las funciones del órgano de control de Argentina, la Dirección Nacional de Protección de Datos Personales, el artículo 29.5 del Decreto de la Ley también prevé:

"Son funciones de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, además de las que surgen de la Ley Nº 25.326:

a) dictar normas administrativas y de procedimiento relativas a los trámites registrales y demás funciones a su cargo, y las normas y procedimientos técnicos relativos al tratamiento y condiciones de seguridad de los archivos, registros y bases o bancos de datos públicos y privados;
b) atender las denuncias y reclamos interpuestos en relación al tratamiento de datos personales en los términos de la Ley Nº 25.326;
c) percibir las tasas que se fijen por los servicios de inscripción y otros que preste;
d) organizar y proveer lo necesario para el adecuado funcionamiento del Registro de archivos, registros, bases o bancos de datos públicos y privados previsto en el artículo 21 de la Ley Nº 25.326;
e) diseñar los instrumentos adecuados para la mejor protección de los datos personales de los ciudadanos y el mejor cumplimiento de la legislación de aplicación;
f) homologar los códigos de conducta que se presenten de acuerdo a lo establecido por el artículo 30 de la Ley Nº 25.326, previo dictamen del Consejo Consultivo, teniendo en cuenta su adecuación a los principios reguladores del tratamiento de datos personales, la representatividad que ejerza la asociación y organismo que elabora el código y su eficacia ejecutiva con relación a los operadores del sector mediante la previsión de sanciones o mecanismos adecuados."

Con carácter general, además de la función de control de los órganos de control, la norma española y argentina prevén una potestad sancionadora.

La norma canadiense, al igual que la española y mexicana, contempla una potestad de los órganos de control que no queda reflejada en los mismos términos en la legislación argentina. Se trata de la potestad de inspección de los sistemas de datos personales para comprobar el cumplimiento de la normativa en materia de protección de datos, mientras que en Argentina esta potestad es dependiente de la autorización judicial.

Hay que reseñar una función de los órganos de control que sólo efectúan la Agencia Española de Protección de Datos y el Instituto Federal de Acceso a la Información Pública (aunque, en este sentido, reiteramos que es necesario tener presente que el IFAI no es exactamente una APD) y que consiste en la potestad de inmovilizar los sistemas de datos personales en caso de incumplimiento de la normativa[47].

En México el órgano de control, denominado *Instituto Federal de Acceso a la Información Pública*, se regula en el artículo 37 de la LAI que le atribuye las siguientes funciones:

> *"I. Interpretar en el orden administrativo esta Ley, de conformidad con el Artículo 6;*
> *II. Conocer y resolver los recursos de revisión interpuestos por los solicitantes;*
> *III. Establecer y revisar los criterios de clasificación, desclasificación y custodia de la información reservada y confidencial;*
> *IV. Coadyuvar con el Archivo General de la Nación en la elaboración y aplicación de los criterios para la catalogación y conservación de los documentos, así como la organización de archivos de las dependencias y entidades;*
> *V. Vigilar y, en caso de incumplimiento, hacer las recomendaciones a las dependencias y entidades para que se dé cumplimiento a lo dispuesto en el Artículo 7;*
> *VI. Orientar y asesorar a los particulares acerca de las solicitudes de acceso a la información;*
> *VII. Proporcionar apoyo técnico a las dependencias y entidades en la elaboración y ejecución de sus programas de información establecidos en la fracción VI del Artículo 29[48];*
> *VIII. Elaborar los formatos de solicitudes de acceso a la información, así como los de acceso y corrección de datos personales;*

[47] Así lo prevé el Lineamiento cuadragésimo primero.
[48] En este mismo sentido el Lineamiento quinto prevé: *Quinto. En cada dependencia o entidad, el Comité de Información señalado en el Artículo 29 de la Ley coordinará y supervisará, a través de la Unidad de Enlace, las acciones de manejo, mantenimiento, seguridad y protección de los sistemas de datos personales.*

IX. Establecer los lineamientos y políticas generales para el manejo, mantenimiento, seguridad y protección de los datos personales, que estén en posesión de las dependencias y entidades;
X. Hacer del conocimiento del órgano interno de control de cada dependencia y entidad, de conformidad con el último párrafo del Artículo 56, las presuntas infracciones a esta Ley y su Reglamento. Las resoluciones finales que al respecto expidan los órganos internos de control y que hayan causado estado deberán ser notificadas al Instituto, quien deberá hacerlas públicas a través de su informe anual;
XI. Elaborar la guía a que se refiere el Artículo 38;
XII. Promover y, en su caso, ejecutar la capacitación de los servidores públicos en materia de acceso a la información y protección de datos personales;
XIII. Difundir entre los servidores públicos y los particulares, los beneficios del manejo público de la información, como también sus responsabilidades en el buen uso y conservación de aquélla;
XIV. Elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de esta Ley;
XV. Cooperar respecto de la materia de esta Ley, con los demás sujetos obligados, las entidades federativas, los municipios, o sus órganos de acceso a la información, mediante la celebración de acuerdos o programas;
XVI. Elaborar su Reglamento Interior y demás normas de operación;
XVII. Designar a los servidores públicos a su cargo;
XVIII. Preparar su proyecto de presupuesto anual, el cual será enviado a la Secretaría de Hacienda y Crédito Público para que lo integre al Presupuesto de Ingresos de la Federación, y
XIX. Las demás que le confieran esta Ley, su Reglamento y cualquier otra disposición aplicable."

En este mismo sentido, hay que tener en cuenta lo previsto en el artículo 62 del Reglamento de la LAI al establecer:

"Sin perjuicio de lo dispuesto por el artículo 37 de la Ley, el Instituto podrá:

I. Diseñar procedimientos y establecer sistemas para que las dependencias y entidades reciban, procesen, tramiten y resuelvan las solicitudes de acceso a la información, así como a los datos personales y su corrección;
II. Establecer sistemas para que las dependencias y entidades puedan enviar al Instituto resoluciones, criterios, solicitudes, consultas, informes y cualquier otra comunicación a través de medios electrónicos, cuya transmisión garantice en su caso la seguridad, integridad, autenticidad, reserva y confidencialidad de la información y genere registros electrónicos del envío y recepción correspondiente;"

Asimismo, los Lineamientos establecen más funciones para el Instituto Federal de Acceso a la Información Pública en su Capítulo VI, titulado *Del Instituto*, que dispone:

"Cuadragésimo. Con objeto de garantizar la protección de datos personales, los sistemas estarán sujetos a la supervisión, inspección y vigilancia del Instituto, teniendo como límite la

materia de estos Lineamientos, por lo que las dependencias y entidades deberán proporcionar la información que el Instituto les requiera, a fin de cumplir respectivamente con sus funciones, en términos de estos Lineamientos.

Cuadragésimo primero. El Instituto podrá ordenar a las dependencias y entidades, como medida precautoria, la suspensión temporal o definitiva del tratamiento de datos personales cuando no se cumplan las medidas técnicas y administrativas establecidas en estos Lineamientos.

Cuadragésimo segundo. A petición del titular, el Instituto podrá requerir la exhibición de la autorización del tratamiento suscrita por el mismo, cuando éste la haya previamente solicitado a la dependencia o entidad y la misma le haya sido negada.

Cuadragésimo tercero. El Instituto no tendrá acceso a los datos personales de un individuo, salvo que medie autorización de su titular, o bien, se requiera supervisar que los sistemas cumplen con los niveles de seguridad en su manejo y tratamiento.

Cuadragésimo cuarto. Asesorar a las dependencias o entidades públicas en la materia de protección de datos personales, así como hacer las recomendaciones conducentes para que se dé cumplimiento a lo dispuesto.

Cuadragésimo quinto. En caso de que alguna dependencia o entidad incurra en irregularidades en el cumplimiento de los presentes Lineamientos, el Instituto podrá hacer del conocimiento del Órgano Interno de Control de las mismas, a efecto de que determine lo conducente con relación a los funcionarios públicos presuntamente responsables."

Conclusiones: en todas las normas analizadas, salvo en el Convenio 108 del Consejo de Europea que no contiene referencia alguna, se prevé la existencia de un órgano de vigilancia y control, sin perjuicio de las atribuciones específicas que la Ley le atribuya en su caso. No obstante, la denominación de dicho órgano varía de unas a otras. En la propia LAI se atribuyen determinadas funciones al Instituto Federal de Acceso a la Información Pública Gubernamental (IFAI), si bien no puede concluirse que sea una autoridad o Agencia de Protección de Datos en el sentido al que se refieren las normas analizadas.

Al establecer una autoridad de control es necesario tener en consideración diferentes aspectos que van a determinar su composición y funciones. En concreto, debe atenderse a la persona o personas que vayan a estar al frente de dicho órgano, pudiendo ser una presidencia o dirección unipersonal o un órgano colegiado; a la existencia de un Registro que gestione las inscripciones de sistemas de datos de carácter personal así como el desarrollo de otras funciones que se le encomienden.

8. PROCEDIMIENTOS

Si el ciudadano considera que sus datos no son tratados correctamente y cree que debe ser tutelado en sus derechos, puede acudir al órgano de control de cumplimiento de la ley, a solicitar que se atiendan sus reclamaciones encaminadas a hacer efectivo y real el cumplimiento de la norma por el titular del sistema de datos personales.

De entre estos procedimientos que las normas a nivel internacional sobre protección de datos contemplan en vía administrativa señalamos por su interés el procedimiento de tutela de derechos y el procedimiento sancionador.

8.1. Procedimiento de tutela de derechos

El ejercicio de los derechos que otorga a los ciudadanos la ley se lleva a cabo mediante un procedimiento de tutela, que podemos orientar en la línea de lo que se ha dado en llamar el "habeas data", como instrumento que permite facilitar un camino mediante el que el afectado puede ejercer la defensa de los derechos que se pretende proteger.

En el Convenio 108:

El artículo 10 del Convenio 108, en relación con las vulneraciones de la normativa sobre la materia, prevé:

> *"Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo."*

En la Directiva 95/46/CE:

En este sentido, la Directiva 95/46/CE dispone en su artículo 22:

> *"Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate."*

Y en el artículo 24:

"Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva."

LOPD	LEY Nº 25326	PIPED Act
TUTELA DE DERECHOS		
Art. 18	**Art. 33**	
1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia Española de Protección de Datos, en la forma que reglamentariamente se determine. 2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. 3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses. 4. Contra las resoluciones de la Agencia Española de Protección de Datos procederá recurso contencioso-administrativo.	1. La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.	

Art. 17.2 R.D. 1332/94	Art. 34	
El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 5/1992 que se consideran vulnerados.	La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.	
	Art. 35	
	La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.	
	Art. 36	
	Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Procederá la competencia federal: a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales.	
Art. 17.1 R.D. 1332/94	**Art. 37**	
Las reclamaciones de los afectados ante la Agencia Española de Protección de Datos, a que se refiere el artículo 17.1 de la Ley Orgánica 5/1992, se sustanciarán en la forma prevista en el presente artículo.	La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.	

Art. 17.3 R.D. 1332/94	Art. 38	
Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.	1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo. En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen. 2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley. 3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial. 4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate. 5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio.	

Art. 17.4 R.D. 1332/94	Art. 39	
	1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante.	
Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada, dando traslado de la misma a los interesados.	Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente. 2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez.	
	Art. 40	
	1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística. 2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad.	
	Art. 41	
	Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley.	
	Art. 42	
	Contestado el informe, el actor podrá, en el término de tres días,	

	ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días.	
Art. 17.5 R.D. 1332/94	**Art. 43**	
Contra la resolución del Director procederá recurso contencioso-administrativo.	1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia. 2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento. 3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante. 4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto.	

Analizando las mismas normas que en apartados anteriores, puede destacarse que en relación con el procedimiento de tutela de derechos la norma canadiense no establece disposiciones concretas al respecto.

En México el procedimiento ante el Instituto Federal de Acceso a la Información se regula en los artículos 49 a 60 de la LAI. En concreto, el procedimiento podrá iniciarse ante la negación de acceso a la información o la inexistencia de los documentos solicitados (artículo 49 LAI).

Con independencia del procedimiento de *habeas data* que se siga en cada lugar, hay que destacar que en España este procedimiento se inicia por las actuaciones contrarias a la LOPD y por la denegación, total o parcial, del ejercicio de los derechos de acceso, rectificación, cancelación y oposición (artículo 18.2 LOPD). En Argentina la acción procederá cuando, por un lado, se quiera conocer cuáles son los datos que se almacenan y con qué finalidad y, por otro, si el tratamiento de los datos no cumple con lo dispuesto en la

legislación argentina o está prohibido por la misma (artículo 33.1 Ley Nº 25326).

8.2. Procedimiento sancionador

El procedimiento sancionador se inicia de oficio por el órgano de control, bien cuando haya tenido conocimiento por denuncia del afectado o de un tercero, o por otros motivos o actos, como puede ser el ejercicio de la actividad inspectora, siendo su objeto comprobar si unos hechos han ocurrido y, en caso de ser constitutivos de una infracción, imponer la correspondiente sanción al responsable del tratamiento o, en su caso, al encargado del tratamiento.

En el Convenio 108:

El Convenio 108 en su artículo 10 establece:

> *"Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo."*

En la Directiva 95/46/CE:

El artículo 24 de la Directiva 95/46/CE dispone:

> *"Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva."*

En las normas nacionales:

LOPD	LEY Nº 25326	PIPED Act
PROCEDIMIENTO SANCIONADOR		
Art. 48		**Division 2**

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título. 2. Las resoluciones de la Agencia Española de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa. 3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses.		12. (2) The Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation. (…) 11. (3) A complaint that results from the refusal to grant a request under section 8 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be.
		Schedule 1
		4.10. An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.
		4.10.1. The individual accountable for an organization's compliance is discussed in Clause 4.1.1.
		4.10.2. Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.
		4.10.3. Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.
		4.10.4. An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

Art. 18 R.D. 1332/94	Art. 31 Decreto	Division 2
Iniciación e instrucción 1. El procedimiento sancionador previsto en el artículo 47 de la Ley Orgánica 5/1992, se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia de un afectado o afectados, por acuerdo del Director de la Agencia Española de Protección de Datos, en el cual se designará instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos. En el referido acuerdo se identificará a la persona o personas presuntamente responsables y se concretarán los hechos imputados, con expresión de la infracción presuntamente cometida y de la sanción o sanciones que pudieran imponerse, así como de las medidas provisionales que, en su caso, se adopten.	3. El procedimiento se ajustará a las siguientes disposiciones: a) La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones de la Ley Nº 25.326 y sus normas reglamentarias, de oficio o por denuncia de quien invocare un interés particular, del Defensor del Pueblo de la Nación o de asociaciones de consumidores o usuarios.	11. (1) An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule 1. 11. (2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter. 12. (3) The Commissioner may delegate any of the powers set out in subsection (1) or (2). 12. (5) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(d). 12. (2) [...] The Commissioner shall give notice of a complaint to the organization against which the complaint was made.
		15. The Commissioner may, in respect of a complaint that the Commissioner did not initiate, (a) apply to the Court, within the time limited by section 14, for a hearing in respect of any matter described in that section, if the Commissioner has the consent of the complainant; (b) appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or (c) with leave of the Court, appear as a party to any hearing applied for under section 14.

2. El acuerdo de incoación del expediente se notificará al presunto responsable y en el mismo se informará a éste de su derecho a formular alegaciones y utilizar los medios de defensa procedentes y que la autoridad competente para imponer, en su caso, la sanción es el Director de la Agencia Española de Protección de Datos, con cita expresa del presente artículo y del artículo 36, g), en relación con el artículo 35, ambos de la Ley Orgánica 5/1992.	b) Se procederá a labrar acta en la que se dejará constancia del hecho denunciado o verificado y de la disposición presuntamente infringida. En la misma acta se dispondrá agregar la documentación acompañada y citar al presunto infractor para que, dentro del plazo de CINCO (5) días hábiles, presente por escrito su descargo y ofrezca las pruebas que hacen a su derecho. Si se tratare de un acta de inspección, en que fuere necesaria una comprobación técnica posterior a los efectos de la determinación de la presunta infracción y que resultare positiva, se procederá a notificar al presunto responsable la infracción verificada, intimándolo para que en el plazo de CINCO (5) días hábiles presente por escrito su descargo. En su primera presentación, el presunto infractor deberá constituir domicilio y acreditar personería. La constancia del acta labrada conforme a lo previsto en este artículo, así como las comprobaciones técnicas que se dispusieren, constituirán prueba suficiente de los hechos así comprobados, salvo en los casos en que resultaren desvirtuados por otras pruebas.	12. (1) The Commissioner shall conduct an investigation in respect of a complaint and, for that purpose, may (a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record; (b) administer oaths; (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law; (d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises; (e) converse in private with any person in any premises entered under paragraph (*d*) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and (f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (*d*) that contain any matter relevant to the investigation.
3. Dentro de los quince días siguientes a la notificación del acuerdo de incoación, el instructor ordenará, de oficio, la práctica de cuantas pruebas y actos de instrucción sean adecuados para esclarecer los hechos y determinar las responsabilidades susceptibles de sanción. En idéntico plazo, el presunto responsable podrá formular las alegaciones y	c) Las pruebas se admitirán solamente en caso de existir hechos controvertidos y siempre que no resulten manifiestamente inconducentes. Contra la resolución que deniegue medidas de prueba sólo se concederá recurso de reconsideración. La prueba deberá producirse dentro del término de DIEZ (10) días hábiles, prorrogables cuando	12. (4) The Commissioner or the delegate shall return to a person or an organization any record or thing that they produced under this section within ten days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

proponer las pruebas que considere convenientes. 4. Transcurrido el plazo previsto en el apartado anterior, el instructor acordará la práctica de las pruebas que estime pertinentes, a cuyo efecto concederá un plazo de treinta días, transcurrido el cual el expediente se pondrá de manifiesto al presunto responsable para que, en el plazo de quince días, formule alegaciones y aporte cuantos documentos estime de interés.	haya causas justificadas, teniéndose por desistidas aquellas no producidas dentro de dicho plazo por causa imputable al infractor.	
Art. 19 R.D. 1332/94	**Art. 31 Decreto**	**División 2**
1. Cumplimentados los trámites previstos en el artículo anterior, el instructor formulará propuesta de resolución motivada en la cual se fijarán de modo claro y preciso los hechos, se razonará, en su caso, la denegación y de la práctica probatoria propuesta por el presunto responsable, se valorarán jurídicamente aquéllos a fin de determinar la infracción cometida y se señalará la sanción a imponer, determinando su cuantía con arreglo a los criterios establecidos en el artículo 44.4 de la Ley Orgánica 5/1992, o bien, se propondrá la declaración de no existencia de responsabilidad.		13. (1) The Commissioner shall, within one year after the day on which a complaint is filed or is initiated by the Commissioner, prepare a report that contains (a) the Commissioner's findings and recommendations; (b) any settlement that was reached by the parties; (c) if appropriate, a request that the organization give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken; and (d) the recourse, if any, that is available under section 14.

2. La propuesta de resolución se notificará al presunto responsable para que, en el plazo de quince días, pueda formular nuevas alegaciones si lo considera oportuno.		13. (3) The report shall be sent to the complainant and the organization without delay. 13. (2) The Commissioner is not required to prepare a report if the Commissioner is satisfied that (a) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available; (b) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province; (c) the length of time that has elapsed between the date when the subject-matter of the complaint arose and the date when the complaint was filed is such that a report would not serve a useful purpose; or (d) the complaint is trivial, frivolous or vexatious or is made in bad faith. If a report is not to be prepared, the Commissioner shall inform the complainant and the organization and give reasons.
3. Notificada la propuesta de resolución o expirado el plazo de alegaciones previsto en el apartado anterior, el instructor elevará el expediente completo al Director de la Agencia Española de Protección de Datos.		
4. El Director podrá, antes de dictar resolución, ordenar al instructor la práctica de cuantas actuaciones considere necesarias, lo que se llevará a efecto en un plazo máximo de quince días.		

5. La resolución, que se dictará dentro de los diez días siguientes, determinará con la necesaria precisión los hechos imputados, la infracción cometida, con expresión del precepto que la tipifique, el responsable de la misma y la sanción impuesta, o bien, la declaración de no existencia de responsabilidad. Contendrá, asimismo, la declaración pertinente en orden a las medidas provisionales adoptadas durante la tramitación del procedimiento.	Concluidas las diligencias sumariales, se dictará la resolución definitiva dentro del término de VEINTE (20) días hábiles.	14. (1) A complainant may, after receiving the Commissioner's report, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1, in subsection 5(3) or 8(6) or (7) or in section 10. (2) The application must be made within forty-five days after the report is sent or within any further time that the Court may, either before or after the expiry of those forty-five days, allow. (3) For greater certainty, subsections (1) and (2) apply in the same manner to complaints referred to in subsection 11(2) as to complaints referred to in subsection 11(1).
6. La resolución se notificará al responsable, con expresión de su derecho a interponer recurso contencioso-administrativo, el plazo de interposición, y el órgano ante el cual deba ser presentado.		
7. Si el procedimiento se hubiera iniciado como consecuencia de denuncia de un afectado, la resolución deberá ser notificada al firmante de la misma.		
		17. (1) An application made under section 14 or 15 shall be heard and determined without delay and in a summary way unless the Court considers it inappropriate to do so. (2) In any proceedings arising from an application made under section 14 or 15, the Court shall take every reasonable precaution, including, when appropriate, receiving representations ex parte and conducting hearings in camera, to avoid the disclosure by the Court or any person of any information or other material that the organization would be authorized to refuse to disclose if it were requested under clause 4.9 of Schedule 1.

		16. The Court may, in addition to any other remedies it may give, (a) order an organization to correct its practices in order to comply with sections 5 to 10; (b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (*a*); and (c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Tal y como queda reflejado en la tabla anterior, España, Argentina y Canadá disponen de un procedimiento sancionador, cuyo desarrollo y ejecución es diferente a causa de los regímenes normativos imperantes en cada país y que, según se ha contrastado, en México no se ha establecido un procedimiento sancionador.

La importancia del procedimiento sancionador reside en que a través del mismo puede hacerse efectivo el cumplimiento de la normativa de protección de datos, lo que constituye una garantía para el titular de los datos, ya que de otro modo el deber de cumplir con lo previsto en dicha normativa pierde todo sentido porque su obligatoriedad no se ve respaldada por medidas que impongan a los responsables su cumplimiento, ya sean medidas económicas, administrativas o de otro tipo.

En definitiva, a través de las medidas adecuadas como las sanciones y recursos convenientes contra la vulneración de la normativa en materia de protección de datos se va a garantizar su plena aplicación.

Conclusiones: si recordamos el triángulo con el que hemos representado gráficamente la protección de datos, es necesario que se establezcan procedimientos que permitan garantizar el cumplimiento de la normativa sobre protección de datos. En este sentido, hemos analizado los procedimientos de tutela de derechos y sancionador, dirigido el primero a tutelar al interesado cuyos derechos no han sido atendidos convenientemente por el responsable del sistema de datos personales y el segundo a comprobar si unos hechos determinados son constitutivos o no de infracción alguna.

En el caso de la normativa mexicana se encuentra amparo ante el IFAI cuando los derechos de modificación o supresión de los datos no son atendidos en la forma exigida por la normativa vigente.

9. RÉGIMEN SANCIONADOR

Tal y como hemos indicado en el apartado anterior, el procedimiento sancionador puede terminar con la imposición de una sanción (económica, administrativa o de otro tipo), si quien trata datos de carácter personal, ya sea el responsable del tratamiento o el encargado del tratamiento, incumple con las obligaciones que le son exigibles en virtud de la normativa sobre protección de datos, incurriendo su acción u omisión en alguna de las infracciones tipificadas en la Ley.

Es decir, la tipificación de conductas que supongan la comisión de una infracción, con su correspondiente sanción, es una garantía para los interesados cuyos datos son objeto de tratamiento, siendo además éste uno de los elementos que tienen estar presentes en un sistema de datos de carácter personal.

En el Convenio 108:

El Convenio 108 en su artículo 10 establece:

> *"Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo."*

En la Directiva 95/46/CE:

El artículo 24 de la Directiva 95/46/CE dispone:

> *"Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva."*

En las normas nacionales:

En la LOPD, la ley Argentina y la sección 28 de la Ley canadiense. No nos detendremos demasiado por ser un apartado absolutamente específico de cada país, y, en consecuencia, poco exportable, en el sentido de su aplicabilidad a otro ordenamiento jurídico diferente.

En la LAI:

Por su parte, la LAI prevé como causas de responsabilidad las acciones y omisiones que se indican en el artículo 63, y que son las siguientes:

> I. Usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente y de manera indebida información que se encuentre bajo su custodia, a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
> II. Actuar con negligencia, dolo o mala fe en la sustanciación de las solicitudes de acceso a la información o en la difusión de la información a que están obligados conforme a la Ley;
> III. Denegar intencionadamente información no clasificada como reservada o no considerada confidencial conforme a la Ley;
> IV. Clasificar como reservada, con dolo, información que no cumple con las características señaladas en la Ley. La sanción sólo procederá cuando exista una resolución previa respecto del criterio de clasificación de este tipo de información del Comité, el Instituto, o las instancias equivalentes previstas en el artículo 61;
> V. Entregar información considerada como reservada o confidencial conforme a lo dispuesto por la Ley;
> VI. Entregar intencionadamente de manera incompleta información requerida en una solicitud de acceso, y
> VII. No proporcionar la información cuya entrega haya sido ordenada por los órganos a que se refiere la fracción IV anterior o el Poder Judicial de la Federación.

La responsabilidad por el incumplimiento de alguna de las obligaciones establecidas en la LAI será exigida conforme a lo dispuesto en la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos. Llama la atención que las sanciones se refieren a la información, pues, tenemos que decir que la LAI sólo destina un capítulo, de 7 artículos, y algunas referencias más dispersas, a la protección de datos, y en este tema es incluso más significativo.

10. CONCLUSIONES

El informe sobre Protección de Datos que hemos realizado en interés del IFAI da lugar a las conclusiones que a continuación se presentan por cada uno de los apartados en los que se divide. Con carácter previo a su exposición, es necesario tener en consideración que México carece de una norma específica que regule la protección de datos de carácter personal con carácter general, si bien en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, promulgada el 17 de febrero de 1917, establece que *"nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones"*.

Lo anterior supone que la LAI no pueda ser considerada como una norma que regula la protección de datos personales directamente, sino que los artículos que en ella se contienen al respecto son una garantía para los ciudadanos como consecuencia de la necesidad de preservar su privacidad en el acceso a la información pública gubernamental que es manejada por la Administración Pública Federal (APF). En este sentido, el objeto de la LAI es *"garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal"* (art. 1), encontrándose su fundamentación constitucional en el artículo 6 (que garantiza el derecho de acceso a la información) y no el artículo 16 (que garantiza la privacidad de los ciudadanos), a pesar de que la LAI sí contiene la regulación relativa al tratamiento de datos de carácter personal por la Administración Pública.

Además, tal y como veremos, es necesario tener en consideración determinados aspectos que llevarían a establecer lo que podemos denominar un "sistema de protección de datos", y que tendrá que ser elaborado por quienes tengan competencia para ello según las diferentes opciones que se presentan a partir del análisis comparativo de la normativa internacional en la materia. En cualquier caso, deben tenerse en consideración todos los factores presentes a la hora de alcanzar un elevado grado de protección de los ciudadanos en la garantía de sus derechos, y en particular de su derecho a la

privacidad en el tratamiento de datos personales, así como la necesidad de alcanzar un nivel adecuado de protección de datos que facilite las transferencias de datos personales desde Estados miembros de la Unión Europea.

0. INTRODUCCIÓN.

De todo lo expresado en el apartado de introducción hay que destacar los siguientes aspectos:

- **Estructura del informe:** a efectos de concretar el análisis en protección de datos que se ha llevado a cabo para el IFAI, el estudio abarca, por un lado, la regulación que a nivel internacional hacen el Convenio (108) del Consejo de Europa, para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, de 28 de enero de 1981, y la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y, por otro lado, algunas legislaciones nacionales que pueden servir como referente a la hora de desarrollar una normativa específica en México, y en concreto, las normas de Argentina, Canadá y España.

  En todo momento la estructura del informe sigue un análisis comparativo, de manera que se analiza primero la regulación hecha por las normas internacionales y nacionales citadas anteriormente, y posteriormente se atiende a la situación actual a nivel federal en México, y más en concreto en la LAI y en el proyecto de Lineamientos sobre Protección de Datos Personales, para, por último, establecer semejanzas y diferencias que permitan atender a la necesidad o no de adoptar medidas concretas para regular la protección de datos de carácter personal, presentándose éstas en cualquier caso como alternativas u opciones legislativas a tener en consideración por quién tenga que tomar la decisión última.

- **Concepto de protección de datos:** por protección de datos debemos entender: *«el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad».*

  Que la protección de datos implica que el titular de los datos es el único que puede decidir cuándo, dónde, cómo y por quién se tratan sus datos de carácter personal. Llegamos así al denominado derecho a la «autodeterminación informativa», que significa que el interesado tiene el control sobre el tratamiento de sus datos de carácter personal, si bien con las condiciones que establezca la normativa sobre protección de datos.

  Aunado a lo anterior, los datos personales se deben tratar conforme a los principios de la protección de datos, que se analizan en el apartado correspondiente del informe, y de manera que se facilite el ejercicio de los derechos de la protección de datos de los ciudadanos, tal y como veremos en su momento. Por último, los principios y los derechos no tendrían sentido sin la previsión de procedimientos que garanticen la tutela de los derechos reconocidos a todo ciudadano y que se sancione a quienes vulneren la normativa sobre protección de datos.

- **Establecimiento de una regulación sobre protección de datos:** el desarrollo de la previsión contenida en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos supone, en primer lugar, atender a la diferencia de tratamiento que se da en el ordenamiento jurídico europeo y en el anglosajón (referido principalmente a Estados Unidos). En el primer caso se caracteriza por la regulación legal de la protección de datos, previéndose sanciones para aquellos responsables de sistemas de datos personales (responsables de sistemas de datos personales o del tratamiento), que incumplan las obligaciones que tienen. En el segundo caso, se parte de una práctica inexistencia de

normas legales sobre la protección de datos, caracterizándose por la denominada "autorregulación industrial" que se basa en el establecimiento de códigos éticos o de conducta, principalmente por parte del sector privado, y cuya efectividad depende en gran medida del poder coactivo de quien desarrolla estos códigos y de la aplicación de las sanciones que en ellos se prevén. No obstante, tal y como ocurre en el ámbito europeo, es posible establecer una regulación específica que garantice a los ciudadanos su derecho a la protección de datos personales, convirtiéndose los códigos éticos en un instrumento adecuado para reforzar, en su caso, esta protección o atender a las especificidades propias de un sector de actividad para la aplicación de la normativa.

- Sistema completo de protección de datos: con este concepto queremos referirnos a la necesidad de que el desarrollo de una norma sobre protección de datos de carácter personal contenga los siguientes aspectos: derechos de las personas, obligaciones del responsable del tratamiento, sanciones apropiadas para quienes incumplan las obligaciones y un organismo de supervisión independiente (conocido como Autoridad o Agencia de Protección de Datos). A partir de aquí, debe atenderse a las particularidades propias de cada normativa con el fin, en todo momento, de garantizar un elevado grado de protección de datos al mismo tiempo que se garantiza, también, la libre circulación de datos para el cumplimiento de los fines legítimos tanto del sector público como del sector privado.

1. GENERALIDADES.

Respecto de las cuestiones generales a tener en consideración en el establecimiento de una norma que regule la protección de datos es necesario atender a los siguientes aspectos:

- **Sujetos de la protección:** a efectos de desarrollar una norma que regule la protección de datos de carácter personal, el legislador debe tener en consideración que su objeto será, precisamente, garantizar el derecho a la privacidad de los ciudadanos, o como también se les denomina en ocasiones "interesados", "afectados" o "titulares de los datos", siendo este derecho una concreción del derecho a la intimidad, en general, y del derecho a la privacidad, en particular. En concreto, es necesario atender aquí al ámbito de aplicación de la norma.

- **Ámbito de aplicación:** al establecer el ámbito de aplicación de la norma sobre protección de datos, el legislador tiene que especificar su ámbito de aplicación objetivo, subjetivo y territorial. En este sentido, en las normas analizadas se identifica un ámbito de aplicación objetivo, en cuanto a que regulan o pueden regular tratamientos automatizados y no automatizados (en papel), así como a que sus disposiciones incluyan tanto sistemas de datos personales de titularidad pública (Administración) como sistemas de datos personales de titularidad privada (sector privado). Por lo que se refiere al ámbito de aplicación subjetivo, debe atenderse a si la protección conferida es sólo para las personas físicas o también quedan incluidas las personas jurídicas. Por último, el ámbito de aplicación territorial determina dónde se van a aplicar las disposiciones de la norma. En cualquier caso, debe considerarse el establecimiento de excepciones de la aplicación de la norma así como la atención a especificidades propias del ordenamiento jurídico en el que se incluye esta normativa.

- **Definiciones:** por último, se analizan las definiciones contenidas en algunas normas y que permiten conocer el alcance de los términos empleados por la normativa analizada. No obstante, es necesario tener en consideración que si bien el establecimiento de definiciones en una norma puede restringir su interpretación, en las normas de nuevas tecnologías en particular, con múltiples conceptos técnicos aparejados, devienen no sólo útiles, sino, en ocasiones, imprescindibles, y, en este sentido, la LAI, y los Lineamientos sobre protección de datos

personales, en concreto, incluyen algunas definiciones que permiten conocer o concretar determinados aspectos de su aplicación.

2. PRINCIPIOS DE LA PROTECCIÓN DE DATOS.

Los principios de la protección de datos, que deben cumplirse en las tres fases en las que puede dividirse el tratamiento de datos personales (recabar los datos, tratar los datos y utilizar y, en su caso, comunicar los datos) son los siguientes:

2.1. Principio del consentimiento

- **Significado:** como regla general es importante establecer que para el tratamiento de los datos personales de los interesados se necesita su consentimiento, entendido éste como una manifestación de voluntad inequívoca, libre, expresa e informada. Así vemos cómo en las normas analizadas, el consentimiento es uno de los principios que debe legitimar el tratamiento de datos personales. No obstante, y a pesar de que lo general es comenzar por el principio general del consentimiento del titular, unido al ya mencionado derecho a la autodeterminación informativa, a modo de apunte, diremos que existe alguna otra norma que no parte del consentimiento como tal, como es el caso de la normativa inglesa, aunque, sin embargo, se llega al mismo de forma indirecta, mediante el establecimiento de normas que confluyen en dicho consentimiento.

- **Forma del consentimiento:** debe tenerse en cuenta la forma en que ha de otorgarse el consentimiento, estando aceptada en la legislación internacional sobre protección de datos la posibilidad de que, como norma general, no se exija una forma concreta, de manera que se admite tanto el consentimiento expreso como el tácito, si bien en este segundo caso se plantea la necesidad de probar que el consentimiento ha sido obtenido por el responsable del tratamiento.

Además, encontramos normas, que, si bien siguen esa regla general de no necesidad de forma alguna, en las que la forma de otorgar el consentimiento puede variar en función de la categoría de datos cuyo tratamiento se esté autorizando por el interesado. Así, por ejemplo, para el tratamiento de datos especialmente protegidos, tales como los relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, puede requerirse que el tratamiento sea expreso y, en su caso, por escrito, siendo este requisito una manifestación del mayor grado de protección que requieren estos datos dada su naturaleza.

- **Necesidad del consentimiento:** las normas analizadas exigen que se obtenga, como norma general, el consentimiento de los interesados para el tratamiento de sus datos personales, si bien también contemplan determinadas excepciones en casos previstos expresamente por la Ley en los que dicho consentimiento no es necesario, como por ejemplo cuando una ley así lo disponga, se trate de datos obtenidos de fuentes de acceso público, tratamientos en interés del titular de los datos, estudios estadísticos y similares. En este sentido, y como mera puntualización, puede ser relevante prever que si se establece que el consentimiento para el tratamiento de los datos pueda ser revocado por el interesado, es necesario que dicha revocación no tenga efectos retroactivos

Por último, es necesario tener en consideración que actualmente la LAI no establece nada sobre la obtención del consentimiento para el tratamiento de datos personales, salvo en lo relativo a la difusión, distribución o comercialización que será analizado en el apartado de cesión o comunicación de datos a terceros, pues entramos ya en la tercera fase del tratamiento, pero no se establece dichas puntualizaciones desde el momento de la recogida. Como ya hemos mencionado, la ausencia del principio del consentimiento es propia del ordenamiento jurídico anglosajón, en el que se llega a este principio a través de la garantía del resto de principios que tienen que cumplirse en

la protección de datos, si bien, en nuestra opinión, resulta aconsejable que en aras a garantizar la seguridad jurídica, tanto para los ciudadanos como para quienes tratan datos de carácter personal, se establezca disposiciones específicas sobre este principio.

2.2. Principio de calidad de los datos

- Todas las normas analizadas, incluida la LAI, contienen previsiones sobre el principio de calidad de los datos, que supone que los datos personales de los interesados sólo puedan tratarse cuando sean adecuados, pertinentes y no excesivos en relación con la finalidad o los propósitos para la que los datos hayan sido obtenidos. Aunado a esto, la finalidad o propósito con el que se traten los datos tiene que ser determinada, explícita y legítima.

  Además, este principio implica que los datos no puedan recabarse por medios que resulten fraudulentos o ilegales, debiendo garantizarse a los interesados que el tratamiento de sus datos de carácter personal sea legal y también leal. En cuanto a la regulación del principio de calidad de los datos, debe tenerse en consideración que es uno de los aspectos que plantea un mayor número de conflictos interpretativos, además de que tiene que ser analizado en estrecha relación con el resto de principios de la protección de datos, y en particular con el consentimiento y la información que se proporciona a los interesados.

2.3. Principio de información en la recogida de datos

- Norma general: el principio de información implica que tenga que proporcionarse determinada información a los interesados sobre los propósitos y las finalidades a las que se van a dedicar los tratamientos de sus datos, así como de otros aspectos tales como la existencia del sistema de datos personales, los destinatarios de los datos, la identidad y domicilio del responsable, el carácter obligatorio o facultativo de la respuesta a las preguntas planteadas, las consecuencias de

proporcionar los datos y la negativa de hacerlo, la posibilidad del ejercicio de los derechos de acceso, rectificación o corrección, cancelación o supresión y oposición. El principio de información supone que el interesado esté en disposición de poder controlar el tratamiento de sus datos de carácter personal ya que sólo a través del ejercicio de sus derechos podrá instar al responsable del tratamiento a, por ejemplo, cancelar o modificar sus datos personales, lo cual sólo será posible si el interesado sabe a quién dirigirse. Esta información tendrá que ser proporcionada tanto cuando los datos personales se obtienen directamente del propio interesado cuando como se recaban a través de un tercero.

- **Excepciones:** sin perjuicio del establecimiento de excepciones a la necesidad de informar al interesado que se establezcan expresamente para casos concretos, tiene que garantizarse este principio de información con independencia de cuál sea el medio, electrónico o no, utilizado para recabar los datos de carácter personal.

2.4. Principio de categorías especiales de datos o datos especialmente protegidos

- El análisis de las normas internacionales de protección de datos proporciona criterios suficientes para recomendar que en el desarrollo de una norma que regule la protección de datos de carácter personal se contemplen las diferentes categorías de datos de carácter personal que puedan establecerse atendiendo a su naturaleza e incluyendo al mismo tiempo las previsiones oportunas y necesarias para garantizar su protección mediante, por ejemplo, el reforzamiento del principio de consentimiento al exigir una determinada forma o la adopción de medidas de seguridad específicas.

- Los datos especialmente protegidos constituyen una cuestión fundamental en el establecimiento de una regulación sobre protección de datos, ya que se refieren o pueden referirse a cuestiones íntimas de

los interesados, que son los titulares de los datos, y que determinan la explicación de un régimen jurídico reforzado para su protección. Por ejemplo, son datos especialmente protegidos los relativos a la ideología, afiliación sindical, religión, creencias origen racial, salud, creencias o vida sexual, así como los datos obtenidos con fines policiales sin consentimiento de los interesados.

- La normativa mexicana que analizamos no hace distinción alguna en lo que a datos de carácter personal se refiere. En este sentido, nuestra experiencia y el análisis comparativo que efectuamos nos lleva a recomendar, de cara a elaborar una normativa específica que regule la protección de datos personales, que se considere y que se contemple expresamente que hay datos personales que por la información que contienen de su titular deben ser considerados con especial cautela dado que pueden comprometer al titular en algún sentido o, mejor dicho, que afectan o pueden afectar a su intimidad de una manera especial.

2.5. Principio de seguridad

- **Obligación de adoptar medidas de seguridad:** la seguridad de los datos personales es otro los principios que tiene que estar presente en el tratamiento de los datos personales, refiriéndose ésta a la necesidad de que quienes traten datos de carácter personal, ya sea el responsable del sistemas de datos personales o el encargado del tratamiento, adopten medidas de índole técnica y organizativas necesarias para garantizar la integridad y confidencialidad de la información. Esta obligación de adoptar las medidas de seguridad necesarias para proteger los datos contenidos en los sistemas de datos de carácter personal se encuentra recogida, en particular, en la Directiva 95/46/CE que hace referencia a medidas "apropiadas", y a medidas "técnicas y organizativas adecuadas", matizando la Directiva en este punto la necesidad de que las medidas no sólo sean de carácter técnico sino también de carácter organizativo de las personas implicadas en el tratamiento de datos.

- Estas medidas de seguridad, cuya adopción se prevé en todas las normas internacionales que son objeto de este análisis, es recomendable que se establezcan en atención a la naturaleza de los datos personales que sean objeto de tratamiento, garantizando así la mayor o menor necesidad de proteger su integridad y confidencialidad. En este sentido, cabe señalar que los factores de riesgo que representa el tratamiento y la naturaleza de los datos son los criterios establecidos por la Directiva 95/46/CE para elegir las medidas de seguridad que se van a aplicar, plasmándose en particular en la regulación establecida sobre la materia por la LOPD en España.

- Por último, en este punto, se hace referencia a que las medidas de seguridad que se decida adoptar deberán reflejarse en un documento escrito o en otro medio que permita acreditar su adopción por quien trata los datos de carácter personal.

- Por lo que respecta a los Lineamientos en materia de protección de datos, y sin entrar en el fondo de cada una de las medidas de seguridad exigidas en los mismos, recomendamos observar cómo a diferencia de en algunas de las legislaciones analizadas, y en particular en los casos de España y Canadá, no se establecen diferencias de niveles en las medidas de seguridad, y se fijan unas medidas de seguridad aplicables a cualquier sistema que contenga datos de carácter personal independientemente del tipo de datos que contengan.

- <u>Niveles de medidas de seguridad:</u> la distinción en niveles de medidas de seguridad viene motivada por la propia naturaleza de los datos que se tratan. La propia Directiva 95/46/CE recoge bajo el título "Categorías especiales de datos" datos que contienen una información especialmente "sensible" de sus titulares, para los que exige un tratamiento específico. Así, pueden determinarse varios niveles según la naturaleza de los datos personales que sean objeto de tratamiento, de manera que los datos que requieran una especial protección tendrán

x°que tener también medidas de seguridad de un nivel superior, y viceversa, los que tengan menos peligro, en cuanto a su confidencialidad e integridad, requerirán un menor establecimiento de medidas de seguridad.

En definitiva, la regulación de las medidas de seguridad requiere profundizar en algunas cuestiones tales como su carácter, de índole técnico y organizativo, así como su establecimiento en atención a la naturaleza de los datos que se tratan en el sistema de datos personales.

2.6. Principio de confidencialidad/deber de secreto

- En el desarrollo de una norma que regule la protección de datos personales, y sin perjuicio de las obligaciones que otras normas del ordenamiento jurídico puedan establecer sobre la obligación de secreto o confidencialidad que puedan tener determinadas profesiones, como la de abogado o médico, es necesario incluir este principio de manera que tanto el responsable del sistema de información como quienes traten datos de carácter personal tengan una obligación de secreto sobre estos datos, incluso una vez que su relación con el responsable del sistema de datos personales finalice.

- De este modo y siendo este un principio que no aparece expresamente recogido como tal en la LAI, debemos destacar que supone un deber que debe observarse por toda persona que tenga acceso a los datos, durante todo el tiempo que dure el tratamiento y aun después de que finalice el mismo.

2.7. Principio de comunicación de datos a terceros

- **Regla general:** la regla general en materia de comunicación o cesión de datos es la de la necesidad de consentimiento del interesado o titular de los datos para poder proceder a dicha comunicación de sus datos de carácter personal a un tercero, salvo excepciones, como que la Ley

prevea otra cosa, o se trate de datos recogidos de fuentes accesibles al público, o con el previo consentimiento del afectado o interesado.

Al igual que para recabar datos, en las normas que venimos analizando en este informe, no se indica que este consentimiento deba ser escrito, ni revestir un formalismo determinado, de donde podemos deducir que puede ser tácito[49], salvo en la LAI en que se exige que sea expreso, siempre que podamos de él determinar con claridad la finalidad de la cesión que se consiente. No obstante, se hace necesario de nuevo atender a las excepciones que también existen a esta norma en el caso, por ejemplo, de algunos datos especialmente protegidos en algunas legislaciones.

- El consentimiento expreso, por su parte, presenta la importante ventaja de la prueba del consentimiento, pues el responsable del tratamiento se encuentra con la ventaja de una prueba del mismo ya preestablecida, pero, por otro lado, en nuestra opinión, cerrar toda posibilidad a que ese consentimiento pueda ser válido cuando sea tácito, puede llegar a entorpecer el tráfico jurídico en algunas ocasiones. Por tanto, es recomendable en todo caso el que el responsable del tratamiento tenga prueba del consentimiento si bien debe efectuarse una regulación que lleve a cabo una ponderación entre las garantías adecuadas para el interesado y la necesidad de garantizar la libre circulación de los datos y no entorpecer en demasía el tráfico mercantil.

- Obligaciones del cedente y del cesionario: en la cesión o comunicación de datos es necesario distinguir entre quien cede o comunica los datos (cedente) y el tercero que recibe la cesión o comunicación (cesionario), pudiendo establecerse obligaciones específicas para cada uno de ellos,

[49] Para no provocar errores, diremos que el consentimiento tácito es válido siempre que la ley no diga otra cosa (como es el caso de los datos especialmente protegidos, que analizaremos después), pero no es recomendable el consentimiento tácito por las dificultades de prueba que tiene. Por lo tanto nuestra recomendación es la de acudir al consentimiento tácito solamente en los casos en que sea absolutamente necesario.

sin perjuicio de la obligación común de tratar los datos de forma legal y leal.

- **Excepciones:** una vez analizada la comunicación de datos en las normas analizadas, si bien se establece como regla general la necesidad del consentimiento del titular, ésta encuentra determinadas excepciones. A pesar de que las excepciones son necesarias, hay que tener en cuenta que el principio del consentimiento es el eje alrededor del que gira la normativa en protección de datos (partiendo del tan nombrado principio a la autodeterminación informativa), y, en este sentido, representa una garantía sustancial para el individuo. Por tanto, es necesario atender a los casos que expresamente se prevean en la normativa que regule la protección de datos, y que entre otros podrían ser los casos en que una ley así lo establezca, o cuando la conexión de sistemas de datos personales con los de terceros sea necesaria para el cumplimiento de una relación contractual, etc.

  La previsión de estas excepciones se refiere única y exclusivamente en cuanto al principio del consentimiento, lo que no supone en modo alguno que no se cumpla con otros principios de la protección de datos, y en particular la información. Es decir, puede no requerirse el consentimiento pero sí la información al interesado.

2.8. Acceso a los datos por terceros

- **Concepto de acceso a los datos por terceros:** tanto en la Directiva europea como en la demás normativa analizada, se contempla la figura del encargado del tratamiento, siendo ésta la que surge cuando resulta necesario para prestar un servicio al responsable del tratamiento o del sistema de datos personales y que no es considerada por la ley como una comunicación de datos puesto que el encargado del tratamiento no es responsable del tratamiento de los datos ya que no es cesionario y no decide sobre el tratamiento, en tanto se limite a tratar los datos conforme a las instrucciones dadas por el responsable del tratamiento

al que presta el servicio, procediendo a realizar un tratamiento de datos por un encargo concreto y para una finalidad concreta y determinada y estando legitimado para el tratamiento de datos en tanto en cuanto y mientras cumpla con ese encargo, estando sujeto a la responsabilidad que le fuera exigible en caso de incumplimiento.

- **Previsión contractual:** es conveniente, y además uno de los requisitos más comunes establecidos en las normas que hemos analizado en el presente informe, que esta prestación de servicios quede regulada en un contrato, que conste por escrito o en alguna otra forma que permita acreditar su celebración y contenido, en el que se indiquen las obligaciones que tendrá que cumplir el encargado del tratamiento en el tratamiento de los datos de carácter personal.

- En concreto, si atendemos a los requisitos del artículo 12 de la LOPD en España, que es quizá la norma que más los detalla, el contrato tendrá que contener las instrucciones del responsable del sistema de datos para el tratamiento de datos de carácter personal por el encargado del tratamiento, el compromiso de este último de adoptar medidas de seguridad, que no utilizará los datos con un fin distinto al previsto en el contrato ni los comunicará, ni siquiera para su conservación, a terceras personas, y que una vez que finalice el contrato el encargado del tratamiento tendrá que devolver los datos personales al responsable, así como la documentación o soportes en los que se contengan datos o, en su caso, destruirlos.

3. DERECHOS DE LOS INTERESADOS.

En el apartado relativo a los derechos de los interesados, se llega a las siguientes conclusiones:

- El reconocimiento en una norma sobre protección de datos de derechos a los interesados es una garantía para la protección de su privacidad, puesto que permiten garantizar, o mejor dicho hacer efectiva, la

aplicación de los principios sobre la protección de datos al poder instar al responsable del sistema de datos personales a adecuar el tratamiento de sus datos de carácter personal (de los interesados) a los requisitos que exigen dichos principios.

- El titular del sistema de datos o del tratamiento no cumple solamente con tratar los datos de carácter personal respetando todos los principios recogidos en la norma sino que, además, es necesario que permita y facilite el ejercicio de los derechos por el interesado.

- De este modo, está obligado a estructurar un procedimiento lógico-administrativo que facilite el ejercicio de los derechos de acceso, rectificación, cancelación de los datos y oposición al tratamiento de datos personales, así como a cualquier otro derecho que la normativa reconozca al titular de los datos.

- Respecto del derecho de acceso, los principios básicos que sobre este derecho establece, en particular, la Directiva 95/46/CE son:

  - Debe permitirse un ejercicio del derecho de acceso:

    - Libre,
    - Con una periodicidad razonable,
    - Sin retrasos, cumpliendo el plazo establecidos para la respuesta, y
    - Sin gastos excesivos para el titular de los datos.

  - El derecho de acceso faculta a su titular para conocer la existencia o inexistencia del tratamiento de datos de carácter personal, es decir, el responsable del tratamiento debe responder al ejercicio del derecho de acceso tenga o no datos de carácter personal del interesado en sus sistemas de datos de carácter personal.

- La información mínima que se debe proporcionar como respuesta al derecho de acceso debe hacer referencia a:

  - fines de dichos tratamientos,
  - las categorías de datos a que se refieran,
  - los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos,
  - el origen de los datos,
  - el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas.

- Respecto de la forma de la respuesta se dispone específicamente que debe proporcionarse la respuesta en forma inteligible para el titular de los datos.

- La normativa mexicana se adecua bastante en este punto a lo establecido por la Directiva 95/46/CE, en cuanto al reconocimiento de los derechos de corrección y supresión de los datos. Si bien queda un punto en el que una normativa específica sobre protección de datos podría ser algo más explícita y es el relacionado con el contenido de la información que en respuesta al ejercicio del derecho de acceso se proporciona al interesado. En este sentido, tiene que recordarse que lo que actualmente desarrolla la LAI es el acceso a la información que maneja la Administración Pública Federal, pudiendo ser conveniente que se regule el derecho de acceso a los datos personales que son tratados en los términos anteriormente indicados.

- Los derechos de rectificación o corrección y cancelación o supresión permiten respectivamente al afectado o interesado, titular de los datos, solicitar la rectificación, en los casos de que los datos sean inexactos o incompletos, y la cancelación, cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido registrados. Si los datos que se encuentran en un sistema de datos son inexactos,

incompletos o no existiera, por el motivo que fuera, derecho a su registro por parte del titular del sistema de datos, el afectado podrá ejercer su derecho de rectificación o su derecho de cancelación, según corresponda.

- El derecho de oposición que sólo es reconocido, además de por la Directiva 95/46/CE por la ley española, es el derecho del titular de los datos a oponerse al tratamiento de los mismos, siempre que una ley no disponga lo contrario y cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

- Por último, podrían e incluso deberían incluirse también otros derechos que permiten garantizar de igual modo la privacidad de los interesados cuyos datos son objeto de tratamiento, y que son el derecho de consulta a un Registro público en el que se inscriban o al que se notifiquen los sistemas de datos personales, a pesar de que en cierta medida ya está reconocido en la LAI y desarrollado reglamentariamente, el derecho de impugnación de valoraciones y el derecho a indemnización. Además, desde el punto de vista de la regulación de los derechos, es necesario que el legislador tenga presentes diferentes aspectos tales como la legitimación para su ejercicio y el propio ejercicio de los derechos.

4. OBLIGACIONES DEL RESPONSABLE DEL SISTEMA DE DATOS PERSONALES.

En cuanto a las obligaciones que se imponen al responsable del sistema de datos personales, cabe señalar lo siguiente:

- Debemos considerar las obligaciones que tiene el responsable del sistema de datos personales en cada una de las fases del tratamiento de datos, recogida, tratamiento y utilización y, en su caso, cesión o comunicación de datos. Además, algunas de estas obligaciones también tiene que cumplirlas el encargado del tratamiento, que trata datos por

cuenta del responsable del sistema de datos personales para prestarle un servicio.

- Algunas de las obligaciones más significativas que puede tener el titular del sistema de datos personales son las siguientes:

  - Realizar un tratamiento legal y leal de los datos.
  - Inscribir los sistemas de datos personales en un Registro creado a tal efecto por el órgano de control o Autoridad en materia de protección de datos.
  - Adoptar las medidas de seguridad que, atendiendo a la naturaleza de los datos, al estado de la tecnología y los riesgos a que están expuestos los datos, garanticen la confidencialidad e integridad de la información.
  - Atender el ejercicio de los derechos que se reconocen a los titulares de datos.

- Es recomendable que la legislación específica que se adopte en materia de protección de datos de carácter personal establezca claramente cuáles son las obligaciones de los responsables de sistemas de datos personales, debiendo considerarse además la oportunidad de adoptar otras medidas adicionales, y no necesariamente de carácter legislativo, con el propósito de dar a conocer las obligaciones de la protección de datos y crear así una cultura social en protección de datos basada en la formación e información.

5. TRANSFERENCIA INTERNACIONAL DE DATOS.

Respecto de los movimientos internacionales de datos o la transferencia internacional de datos (en adelante, TID), puede señalarse lo siguiente:

- Por definición, la transferencia internacional de datos (TID) supone que unos datos personales salgan del territorio de aplicación de la norma, siendo necesario que el responsable del tratamiento aporte garantías

suficientes de cara al interesado con el propósito de que este tratamiento de datos no suponga una lesión en su derecho a la privacidad. Además, implica que puedan entrar en conflicto al menos dos ordenamientos jurídicos, de manera que tiene que establecerse una regulación que permita transferir datos a un tercer país con todas las garantías que se cumplirían en el tratamiento de los datos en el territorio en que se aplica dicha norma.

- Atendiendo a la regulación en Europa sobre la TID, la regla general es la de que el país tercero al que se transfieran los datos de carácter personal desde un país sujeto al ámbito de aplicación de la Directiva 95/46/CE, deberá reunir los requisitos necesarios para ser considerado un país que garantiza un nivel de protección adecuado. En este mismo sentido, la LOPD exige un nivel equiparable.

- Por tanto, y de manera esquemática, la clasificación de la TID en la regulación de la Unión Europea puede realizarse con base en dos criterios:

  1º Por el país de destino: en función de cuál sea el país de destino, podemos diferenciar, a su vez, tres casos distintos:

  - Un país de la Unión Europea o del Espacio Económico Europeo[50].
  - Un país declarado con un nivel adecuado de protección (Suiza, Hungría[51], Canadá, entidades adheridas al Acuerdo de Puerto Seguro -Estados Unidos-, Argentina, Bahilía de Guernsey e Isla de Man).
  - Un tercer país respecto del que no se haya declarado el nivel adecuado.

[50] El Espacio Económico Europeo está formado por los Estados miembros de la Unión Europea (Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Irlanda, Italia, Luxemburgo, Países Bajos, Portugal, Reino Unido, Suecia, y los adheridos recientemente, Polonia, Eslovenia, Eslovaquia, Hungría, República Checa, Estonia, Lituania, Letonia, Malta y Chipre) y Noruega, Islandia y Liechtenstein.

[51] Si bien es necesario tener en consideración que Hungría ya es un Estado miembro de la UE.

En los dos primeros casos, la TID puede realizarse del mismo modo que las comunicaciones, o en su caso prestaciones de servicios, dentro del país comunitario origen de los datos. Es decir, no requiere de autorización previa, pudiendo realizarse la transferencia de forma automática por el responsable del sistema de datos establecido en el territorio de algún Estado miembro. En el tercero de los casos, la transferencia no es libre, y requiere acudir a la autorización del organismo de control, o bien a algunas de las excepciones de la normativa, o a la utilización de mecanismos contractuales, entre otros.

2º Por la finalidad con la que se realiza la TID: en función de la finalidad para la que se realiza la TID, ésta puede ser a su vez:

- Una comunicación a un tercero (entre dos responsables de sistemas de datos personales).
- Un encargo o prestación de servicios (entre un responsable del sistema de datos establecido en el territorio de alguno de los Estados miembros de la UE y un encargado del tratamiento establecido en un tercer país).

- En resumen, podrá llevarse a cabo una TID de datos a un país tercero en los siguientes supuestos:

4. Cuando se declare el nivel de protección adecuado en el tercer país receptor de los datos.

5. Cuando se esté en una de las excepciones tasadas en la Directiva, o en las normativas nacionales.

6. Cuando se haga uso de un mecanismo contractual que cumpla las garantías de la protección de datos aunque el país receptor no garantice un nivel de protección adecuado[52].

[52] En este sentido, en la Unión Europea se han aprobado dos Decisiones de la Comisión Europea por la que se establecen clausulados tipo para la transferencia de datos a terceros países en virtud de una cesión o comunicación de datos o de una prestación de servicios por un encargado del tratamiento.

- En conclusión, las transferencias de datos a un país tercero podrán llevarse a cabo cuando:

  - el país tercero destinatario de los datos esté declarado como país que proporciona un nivel adecuado de protección, o
  - el país de destino no proporcione un nivel adecuado de protección y no estemos en una de las excepciones del artículo 26 de la Directiva 95/46/CE, pero se opte por el modelo de contrato propuesto por la Comisión, cuyas cláusulas ofrecerán las garantías respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas y el respeto al ejercicio de los respectivos derechos.

- Siendo la única referencia que encontramos en el texto normativo de los Lineamientos en materia de protección de datos, la realizada en el Lineamiento 24[53], recomendamos considerar, que si bien debe buscarse ese nivel adecuado de protección en los países destinatarios de la TID, sería conveniente regular otras cuestiones que hacen referencia, entre otros aspectos, a:

  - la autoridad que va a ser competente para determinar dicho nivel adecuado,
  - los criterios conforme a los cuales va a considerarse ese nivel adecuado de protección,
  - las excepciones en las que a pesar de no evaluarse el nivel adecuado de protección del país destinatario de la TID va a procederse a realizar la transferencia de datos, por ejemplo, en los casos en los que el titular de los datos consienta la transferencia, dado que siendo el principio de consentimiento uno de los

[53] En caso de que el o los destinatarios de los datos sean personas o instituciones de otros países, las dependencias y entidades deberán asegurarse que tales países garanticen que cuentan con niveles de protección semejantes o superiores a los establecidos en estos Lineamientos, y en la normatividad propia de la dependencia o entidad de que se trate.

principios básicos en materia de protección de datos, el titular de los datos puede de este modo autorizar la transferencia.

- En definitiva, sería conveniente y recomendable que México estableciera previsiones sobre la TID en su normativa sobre protección de datos, por un lado, con el propósito de garantizar el derecho a la privacidad de los interesados y, por otro lado, para conseguir que sea declarado, como ya ocurrido con otros países, un país con nivel adecuado en protección de datos lo que facilitaría, en gran medida, la realización de transacciones comerciales con Estados miembros de la Unión Europea.

6. ÓRGANO DE CONTROL.

Por lo que respecta al órgano de control, al que suele denominarse Autoridad o Agencia de Protección de Datos, cabe señalar lo siguiente:

- En todas las normas analizadas se prevé la existencia de un órgano de vigilancia y control, sin perjuicio de las atribuciones específicas que la Ley le atribuya en su caso. No obstante, la denominación de dicho órgano varía de unas a otras así como su composición, ya que en unos casos es un órgano unipersonal mientras que en otros es un órgano colegiado. En este sentido, es importante que se tengan en consideración estos aspectos a la hora de establecer un órgano de vigilancia y control en materia de protección de datos. Así, en el establecimiento de un órgano de control para el desempeño de determinadas funciones en materia de protección de datos hay que tener en cuenta la persona o personas que vayan a estar al frente de dicho órgano, las competencias que va a desempeñar, cómo se deben ejercer estas funciones y cuáles serán las asignaciones económicas que le correspondan.

- Además, hay que tener en cuenta que en la propia LAI se atribuyen determinadas funciones al Instituto Federal de Acceso a la Información Pública Gubernamental (IFAI), si bien no puede concluirse que sea una

Autoridad o Agencia de Protección de Datos en el sentido al que se refieren las normas analizadas.

- En este sentido, el régimen jurídico al que quede sometido el órgano de control va a depender en gran medida del régimen normativo del país que lo cree, así como el ejercicio de las funciones que tenga atribuidas el órgano de control va a depender del régimen legislativo que impere.

Por último, como principales potestades se pueden destacar, en las normas analizadas, las de control de cumplimiento de la normativa, de inspección de los sistemas de datos personales, de inmovilización de los sistemas de datos y sancionadora.

7. CÓDIGOS DE CONDUCTA.

En relación con los códigos de conducta, tipo, éticos, deontológicos o de buena práctica, cabe señalar lo siguiente:

- Los códigos tipo o códigos de conducta son instrumentos de autorregulación especialmente aptos para adaptar los diversos preceptos de una ley a las características específicas de cada sector, ya sea público o privado dado que pueden ser promovidos y elaborados por cualquiera que quiera establecer una protección superior a la que confieren las normas legales. En este sentido, estos códigos también pueden tener el carácter de códigos deontológicos o de buena práctica profesional, pudiendo constituir un medio a través del cual el titular del sistema de datos pueda ofrecer a los ciudadanos una garantía de conocimiento y cumplimiento de la normativa sobre protección de datos.

- Estos códigos tipo son voluntarios, ya que las partes deciden libremente su adhesión a los mismos, y no tienen carácter de norma jurídica en el sentido de emanar del Poder Legislativo del Estado, sino que son normas autónomas que los sujetos deciden darse a sí mismos para su

propia regulación (autorregulación), generalmente como complemento a la normativa.

Dado que la legislación mexicana analizada no regula los códigos tipo, podría ser una cuestión importante y útil, tanto en el sector público como en el privado, impulsar la elaboración y aplicación de códigos de conducta voluntarios, por ejemplo por las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores. En este sentido, podría establecerse la participación de las asociaciones y organizaciones representativas en la elaboración de estos códigos y, en su caso, incluso la creación de un distintivo que permita identificar a quienes respeten los códigos de conducta que se adopten.

- En definitiva, estos códigos deben proporcionar en todo caso un elevado grado de protección a los interesados, no olvidando que una importante garantía de su cumplimiento se afianzará en gran medida a través de sanciones que tendrán que ser respaldadas por un órgano que tenga poder suficiente para imponerlas y hacerlas cumplir, dependiendo la efectividad del código en gran medida de esto último.

8. PROCEDIMIENTOS.

Los procedimientos garantizan la aplicación práctica de los principios y de los derechos por parte del responsable del sistema de datos personales. En este sentido, en las normas analizadas podemos distinguir principalmente dos clases de procedimientos.

8.1. Procedimiento de tutela de derechos

- Si el ciudadano considera que sus datos no son tratados correctamente y cree que debe ser tutelado en sus derechos, puede acudir al órgano de control de cumplimiento de la ley, a solicitar que se atiendan sus reclamaciones encaminadas a hacer efectivo y real el cumplimiento de la norma por el titular del sistema de datos personales.

- La garantía del ejercicio de los derechos que otorga a los ciudadanos la ley se lleva a cabo mediante un procedimiento de tutela, que podemos orientar en la línea de lo que se ha dado en llamar el "habeas data", como instrumento que permite facilitar un camino mediante el que el afectado puede ejercer la defensa de los derechos que se pretende proteger.

- En el caso de la normativa mexicana se encuentra amparo ante el IFAI cuando los derechos de modificación o supresión de los datos no son atendidos en la forma exigida por la normativa vigente. Esto significa que, en cierta medida, se cuente ya con un procedimiento de tutela de derechos, circunscrito, evidentemente, al ámbito de aplicación de la LAI, es decir, los datos objeto de tratamiento en las dependencias de la Administración Pública.

8.2. Procedimiento sancionador

- En las normas nacionales analizadas, y en particular en la LOPD en el caso de España, el procedimiento sancionador puede iniciarse de oficio por el órgano de control, por denuncia del afectado o por otros motivos o actos, como puede ser el ejercicio de la actividad inspectora con el propósito de determinar si unos hechos son constitutivos de infracción, lo que, en su caso, determinaría la imposición de la correspondiente sanción al infractor en los términos previstos en la ley.

- La normativa mexicana de protección de datos no regula un procedimiento sancionador sobre esta materia, debiendo tenerse en consideración que al desarrollar una norma específica sobre protección de datos sería conveniente que se incluyeran previsiones al respecto.

- Es recomendable prever un procedimiento sancionador para motivar a los responsables del tratamiento en el cumplimiento de la normativa de protección de datos, estando esta cuestión en estrecha relación con las sanciones, tal y como se ve en el siguiente apartado.

9. RÉGIMEN SANCIONADOR.

En cuanto a las sanciones, que constituyen otro de los aspectos que deben estar presentes en un sistema de protección de datos, como garantía para el derecho a la privacidad de los ciudadanos, es necesario tener en consideración lo siguiente:

- La tipificación de conductas que supongan la comisión de una infracción, con su correspondiente sanción, es una garantía para los interesados cuyos datos son objeto de tratamiento, siendo además éste uno de los elementos que tienen estar presentes en un sistema de datos de carácter personal con objeto de salvaguardar su efectividad.

- Es decir, en un sistema de protección de datos se necesita establecer un régimen sancionador con el fin de que los principios básicos establecidos no queden en meros principios teóricos sino que se hagan efectivos.

- En el caso de la LAI, se prevén algunas infracciones para los sujetos obligados que incumplen las obligaciones, siendo conveniente que una regulación normativa sobre la protección de datos establezca infracciones claras con sus correspondientes sanciones en aras a garantizar el cumplimiento de las obligaciones por los responsables de sistemas de datos personales y con ello el derecho a la protección de datos de los interesados.

ANEXO I

Este Anexo tiene como propósito ofrecer una enumeración de los aspectos a tener en consideración en materia de protección de datos en la configuración de una norma específica que regule esta materia. Por ello, a continuación se incluye una tabla en la que, en la columna de la izquierda se indica la cuestión y, en la columna de la derecha, los aspectos que deben tenerse presentes por cada una.

Cuestión	Aspectos a considerar
Objeto	❒ Derecho a la protección de datos personales (derecho a la privacidad).
Ámbito de aplicación	❒ Objetivo ■ Tratamientos automatizados ■ Tratamientos no automatizados (papel) ■ Regímenes especiales ■ Supuestos de exclusión (tratamientos con fines domésticos, materias reservadas, etc.) ❒ Subjetivo ■ Sujetos protegidos: - Personas físicas - Personas morales ■ Sujetos obligados: - Responsable del sistema de datos personales - Encargado del tratamiento ■ Sectores de aplicación: - Sector privado - Sector público (Administración Pública). ❒ Territorial
Definiciones	❒ Datos personales o de carácter personal ❒ Fichero (sistema de datos personales) ❒ Tratamiento de datos ❒ Interesado (afectado o titular de los datos) ❒ Responsable del sistema de datos personales ❒ Encargado del tratamiento ❒ Cesión o comunicación de datos ❒ Procedimiento de disociación ❒ etc.

Cuestión	Aspectos a considerar
Principios de la protección de datos (condiciones de licitud del tratamiento)	❒ Consentimiento ■ Norma general: necesidad ■ Excepciones: tasadas en la Ley ■ Forma del consentimiento: tácito, expreso y, en su caso, por escrito ■ Revocabilidad ❒ Calidad de los datos ■ Adecuados, pertinentes y no excesivos ■ Propósitos expresos y legítimos para el tratamiento de los datos ■ Prohibición de recabar datos por medios desleales o ilícitos ■ Tratamiento legal y leal ❒ Información en la recogida de datos personales ■ Datos recabados del propio interesado ■ Datos recabados de un tercero ■ Información a proporcionar ❒ Datos especialmente protegidos ■ Categorías ■ Especial protección: forma del consentimiento ❒ Medidas de seguridad ■ De índole técnica y organizativas ■ Garantizar la confidencialidad e integridad de la información ■ En atención a la naturaleza de los datos personales ■ Implantación mediante un documento de seguridad ❒ Deber de secreto ❒ Comunicación o cesión de datos ■ Norma general: necesidad del consentimiento ■ Excepciones ■ Forma del consentimiento ■ Revocabilidad del consentimiento ❒ Acceso a los datos por terceros ■ No consideración como cesión de datos ■ Necesidad de que conste en un contrato (contenido del contrato)
Derechos de las personas en la protección de datos	❒ Derecho de consulta al Registro ❒ Derecho de acceso ❒ Derecho de corrección y supresión de datos ❒ Derecho de oposición ❒ Derecho de impugnación de valoraciones ❒ Derecho a indemnización ❒ Requisitos para el ejercicio de los derechos

Cuestión	Aspectos a considerar
Régimen de los ficheros	❒ Notificación/comunicación al Registro público ■ Inscripción, modificación y supresión ■ Ficheros de titularidad pública y privada
Transferencia Internacional de Datos	❒ Norma general: prohibición de transferencias a terceros países sin nivel adecuado ❒ Excepciones a la norma general ❒ Solución contractual ❒ Obtención por México del nivel adecuado otorgado por la Comisión Europea
Procedimientos	❒ Procedimiento de tutela de derechos ❒ Procedimiento sancionador
Órgano de control (Autoridad o Agencia de Protección de Datos)	❒ Denominación ❒ Composición ❒ Funciones y potestades
Régimen sancionador	❒ Sujetos responsables ❒ Infracciones ❒ Sanciones

ANEXO II

El objeto de este Anexo es dar respuesta a dos aspectos concretos del análisis sobre la problemática internacional generada con la entrada en vigor de las Leyes de Protección de Datos de Carácter Personal, y que debe unirse al informe ya entregado con el propósito de complementarlo. Esto significa y supone que nos remitimos por completo a lo ya dicho en el citado Informe, de manera que aquí nos vamos a limitar a desarrollar los aspectos que se indican a continuación.

En primer lugar, atenderemos de manera específica a la reglamentación de las leyes que hemos analizado en el Informe, es decir, de Argentina, Canadá y España, si bien nos centraremos en esta última por ser la que tiene un sistema de protección de datos que puede aproximarse más a las necesidades que pueden plantearse al desarrollar una legislación específica en México y que puede tomarse en consideración como modelo.

En segundo lugar, por cada una de las normas analizadas e indicadas anteriormente, atenderemos a la problemática gubernamental que presentan estas normas en los respectivos ordenamientos jurídicos y al impacto social que éstas tienen.

En ambos casos, y puesto que en nuestro informe hemos analizado también la Directiva 95/46/CE como norma que, en el ámbito europeo, es de obligada transposición para los veinticinco Estados miembros, habiendo prestado aquí especial atención a la transposición realizada por España a través de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), vamos a atender a la regulación establecida en el ámbito de la Unión Europea. Así, en cuanto a la reglamentación de esta Directiva tendremos en consideración algunas normas que, a nivel europeo, regulan determinados aspectos de los tratamientos llevados a cabo por las instituciones comunitarias, y, respecto del impacto social y gubernamental de esta Directiva,

queremos atender, brevemente, a los informes sobre su aplicación emitidos por la Comisión Europea y por el Parlamento Europeo.

Respecto de este último extremo, para la preparación del *"Informe de la Comisión – Primer Informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)"* (COM(2003) 265 final)[54], la Comisión Europea llevó en mayo de 2002 una consulta a los Estados miembros y a las Autoridades nacionales de Protección de Datos con el propósito de conocer las medidas adoptadas para aplicar la Directiva 95/46/CE y conocer las dificultades encontradas. Tanto los Estados miembros como las Autoridades de Protección de Datos respondieron a las cuestiones planteadas conforme a la situación de su normativa interna.

Además de lo anterior, la publicación del informe dio lugar, entre otras acciones, a que se publicaran los resultados de dos encuestas sobre protección de datos en otoño de 2003 *(Eurobarometer surveys on data protection awareness in to the European Union)*, habiéndose realizado una consulta a través de Internet entre los ciudadanos y los responsables de sistemas de datos el 25 de junio de 2002. Se trataba así de conocer el impacto social que la normativa sobre protección de datos tiene entre los ciudadanos europeos.

Toda la información relativa a los trabajos de la Comisión Europea en cuanto a la transposición de la Directiva 95/46/CE por los Estados miembros, las respuestas a la consulta por las Autoridades de Protección de Datos y los resultados de la encuesta realizada entre los ciudadanos y los responsables de sistemas de datos que quisieron responder, la cual consideramos puede ser de interés para el IFAI, se encuentra disponible en http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm. En cualquier caso, para completar nuestro Anexo haremos referencia a la información que resulte imprescindible, por considerar que puesto que se trata de información proveniente de la Comisión Europea y dado que también se encuentran aquí documentos con las respuestas de quienes participaron en las

[54] Disponible en http://europa.eu.int/eur-lex/es/com/rpt/2003/com2003_0265es01.pdf.

consultas, es aconsejable que el IFAI, si lo desea, pueda consultar directamente estos documentos al objeto de sacar sus propias conclusiones sin que nuestro trabajo se extienda más allá de lo necesario y resulte inadecuado a los objetivos que se nos han marcado.

En la medida de lo posible, y con objeto de no extendernos en exceso, nos limitaremos a atender a estas cuestiones.

1. Reglamentación de las Leyes de Protección de Datos

Dentro de este apartado nos vamos a centrar en atender a cuál ha sido el desarrollo reglamentario de las normas estudiadas en el Informe, debiendo entender que por desarrollo reglamentario se entiende todos los aspectos necesarios para la implantación práctica de la normativa sobre protección de datos en el país correspondiente, además de incluir, por último, una referencia a la normativa general sobre protección de datos en la Unión Europea ya que en nuestro Informe hemos analizado la Directiva 95/46/CE como norma de obligado cumplimiento tanto para los Estados miembros como para las instituciones públicas comunitarias.

1.1. ESPAÑA

Mediante la siguiente tabla reflejamos aquellas cuestiones que, reguladas en la LOPD, han sido objeto de desarrollo reglamentario, bien sea a través de un Real Decreto u otra norma, incluyendo las Instrucciones[55] de la Agencia Española de Protección de Datos.

Apartado de la LOPD	Desarrollo reglamentario
En general, articulado de la Ley[56].	❑ Desarrollado por el Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, publicado en el Boletín Oficial del Estado número 147, de 21 de junio. ❑ Instrucción 2/1995, de 4 de mayo, de la Agencia Española de Protección de Datos, relativa a las medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo

[55] Las Instrucciones dictadas por la Agencia Española de Protección de Datos, sin tener carácter normativo, representan la línea interpretativa realizada por el órgano encargado de velar por el cumplimiento de la normativa sobre protección de datos de carácter personal en España.

[56] No obstante, es necesario tener en consideración las cuestiones que se indican en el análisis de esta norma.

	hipotecario o personal, publicada en el Boletín Oficial del Estado número 110, de 9 de mayo. ❑ Instrucción 1/1996, de 1 de marzo, de la Agencia Española de Protección de Datos, relativa a los ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios, publicada en el Boletín Oficial del Estado número 62, de 12 de marzo. ❑ Instrucción 2/1996, de 1 de marzo, de la Agencia Española de Protección de Datos, relativa a los ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo, publicada en el Boletín Oficial del Estado número 62, de 12 de marzo.
Medidas de seguridad (art. 9)	❑ Desarrollado mediante el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, publicado en el Boletín Oficial del Estado número 151, de 25 de junio. ❑ Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas en el Reglamento aprobado por el Real Decreto 994/1999, publicado en el Boletín Oficial del Estado número 49, de 26 de febrero. ❑ Resolución del Ministerio de Justicia, de 22 de junio de 2001, de la Subsecretaría, por la que se dispone la publicación del Acuerdo del Consejo de Ministros por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información, publicada en el Boletín Oficial del Estado número 151, de 25 de junio.
Derechos de las personas: acceso, rectificación y cancelación (artículos 15 y 16)	❑ Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, publicada en el Boletín Oficial del Estado núm. 25, de 29 de octubre.
Prestación de servicios de información sobre solvencia patrimonial y crédito (art. 29)	❑ Instrucción 1/1995, de 1 de marzo, de la Agencia Española de Protección de Datos, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito, publicada en el Boletín Oficial del Estado número 54, de 4 de marzo..
Transferencia internacional de datos (artículos 33 y 34)	❑ Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos, publicada en el Boletín Oficial del Estado número 301, de 16 de diciembre.
Agencia Española de Protección de Datos (art. 35)	❑ Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, publicado en el Boletín Oficial del Estado número 106, de 4 de mayo.

Órganos correspondientes de las Comunidades Autónomas[57]	❑ Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, publicada en el Boletín Oficial del Estado número 245, de 12 de octubre. ❑ Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, publicada en el Boletín Oficial del Estado número 115, de 14 de mayo. ❑ Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, publicada en el Boletín Oficial del País Vasco número 44, de 4 de marzo.
Inscripción de sistemas de datos de titularidad pública y privada (arts. 20 y 25)	❑ Resolución de 30 de mayo de 2000, de la Agencia Española de Protección de Datos, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de las que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos, publicada en el Boletín Oficial del Estado número 153, de 27 de junio.

Este desarrollo normativo tiene que entenderse sin perjuicio de las referencias que, en su caso, pudieran hacerse a otras normas del ordenamiento jurídico español que puedan desarrollar determinados aspectos pero en las que no vamos a entrar por exceder los objetivos de nuestro estudio, piénsese por ejemplo en la exigencia de responsabilidad a los servidores públicos conforme a la normativa específica que regula esta materia, o al desarrollo de determinados aspectos del procedimiento sancionador que determina la necesidad de atender a la normativa de carácter administrativo-sancionador.

A continuación, vamos a explicar brevemente las normas que hemos indicado en la tabla anterior con el propósito de conocer el objeto de cada una de ellas.

1.1.1. Real Decreto 1332/1994

El Real Decreto 1332/1994, anterior a la LOPD, se entiende vigente en virtud de la Disposición transitoria tercera de esta última en tanto no se oponga a la misma y hasta que no se dicte un nuevo Reglamento. Tiene por objeto desarrollar determinados artículos de la LOPD que remiten su desarrollo y

[57] De los cuales únicamente citaremos las leyes que regulan la protección de datos en cada Comunidad Autónoma que ha creado una Agencia de Protección de Datos.

parte de su aplicación práctica al desarrollo reglamentario. Entre otras cuestiones, el articulado del Real Decreto 1332/1994 desarrolla el ejercicio de los derechos de acceso, rectificación y cancelación por el afectado, el modo y forma de efectuar las correspondientes reclamaciones a la Agencia Española de Protección de Datos (AEPD), la notificación e inscripción de sistemas de datos personales en el Registro General de Protección de Datos (RGPD) y el procedimiento sancionador para la determinación de las infracciones y la imposición de las sanciones.

1.1.2. Instrucción 2/1995

La Instrucción 2/1995 nos permite conocer la línea interpretativa de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal, dado que en dichos tratamientos suele haber datos especialmente protegidos, relativos a la salud, que requieren de una mayor protección en las tres fases en las que puede dividirse el tratamiento de los datos, y a las que ya hemos atendido en el Informe al cual ahora nos remitimos.

1.1.3. Instrucción 1/1996

La Instrucción 1/1996 tiene por objeto un tratamiento específico de datos, el relativo a los datos personales que se tratan como consecuencia del control de acceso a edificios, ya sea en centros de trabajo o dependencias públicas, a donde se acude para efectuar actividades relacionadas con las propias del centro visitado. Con esta Instrucción se trata de dar respuesta a las cuestiones concretas que plantea el tratamiento de datos personales en estos sistemas de datos, y que se centran en los datos constituidos por sonido e imagen, los datos necesarios para cumplir con el propósito de vigilancia que determina la existencia de estos sistemas de datos, el consentimiento necesario para ello, el período durante el que se conservarán y su posterior cancelación.

1.1.4. Instrucción 2/1996

Esta Instrucción se dirige a concretar la aplicación de la normativa sobre protección de datos en los sistemas de datos establecidos para controlar el acceso a casinos y salas de bingo, incidiendo especialmente en los principios de información al interesado cuyos datos son objeto de tratamiento, su consentimiento para la cesión o comunicación de datos fuera de los supuestos legalmente previstos y el plazo en que deben cancelarse los datos por dejar de ser necesarios o pertinentes para el propósito con el que fueron recabados.

1.1.5. Real Decreto 994/1999

El Real Decreto 994/1999 ó Reglamento de Medidas de Seguridad desarrolla lo dispuesto en el artículo 9 de la LOPD, relativo al principio de seguridad, y que establece la obligación del responsable del sistema de datos y, en su caso, del encargado del tratamiento, de adoptar las medidas de índole técnica y organizativas para garantizar la seguridad de los datos y que deben implantarse en los sistemas de datos personales, los centros de tratamiento, locales, equipos sistemas, programas y las personas que intervengan en el tratamiento de datos.

En atención a la naturaleza de los datos que son objeto de tratamiento y dada la mayor o menor necesidad de garantizar su confidencialidad e integridad, se establecen tres niveles de medidas de seguridad (básico, medio y alto) que deberán reunir los sistemas de datos personales. Así, el Reglamento de Medidas de Seguridad contempla la necesidad de elaborar un documento de seguridad a través del que el responsable del sistema de datos personales implantará las medidas de seguridad, siendo éste de obligado cumplimiento para el personal que tenga acceso a los datos y a los sistemas de información.

Por último, cabe señalar que el Reglamento preveía unos plazos para que los sistemas de datos preexistentes adoptaran estas medidas de seguridad, siendo éstos el 26 de diciembre de 1999 para los sistemas de datos de nivel básico, el 26 de junio 2000 para los sistemas de datos de nivel medio y el 26 de junio de

2001 para los sistemas de nivel alto. En el caso de los sistemas de datos de nivel básico y alto, posteriormente se publicaron normas para ampliar dichos plazos, tal y como veremos a continuación. En cuanto a los sistemas de información que encontrándose en funcionamiento a la entrada en vigor del Real Decreto 994/1999 no permitieran la implantación de medidas de seguridad el plazo para su adecuación era de tres años, finalizando el 26 de junio de 2002.

1.1.6. Real Decreto 195/2000

Tal y como acabamos de indicar al analizar los plazos para la implantación de las medidas de seguridad previstas en el Real Decreto 994/1999, en ficheros de nivel básico finalizaba el 26 de diciembre de 1999, según la previsión contenida en su Disposición transitoria única. No obstante, en atención al esfuerzo que significó la adecuación de sistemas de información al "efecto 2000", se vio la necesidad de dictar el Real Decreto 195/2000 con el propósito de establecer un nuevo plazo para la implantación de estas medidas, el 26 de marzo de 2000, prorrogando así tres meses el plazo para su adecuación.

1.1.7. Resolución del Ministerio de Justicia de 2001

Al igual que en el caso del Real Decreto 195/2000, pero referido al nivel alto de medidas de seguridad, el Consejo de Ministros, en atención a las dificultades de orden tecnológico que se encontraron por los responsables de sistemas de datos tanto de titularidad pública como privada, decidió conceder una prórroga, de manera que el plazo finalizaría el 26 de junio de 2002 y no el 26 de junio de 2001, coincidiendo así con el plazo inicialmente previsto para los sistemas de información que, a la entrada en vigor del Real Decreto 994/1999, no permitieran la implantación de medidas de seguridad.

1.1.8. Instrucción 1/1998

La Instrucción 1/1998 constituye una guía de la Agencia Española de Protección de Datos, dirigida a los responsables de sistemas de datos

personales de cómo atender al ejercicio de los derechos de acceso, rectificación y cancelación. En la introducción de la Instrucción se indica expresamente que *"tiene por objeto aclarar las disposiciones relativas a los derechos de acceso, rectificación y cancelación, ya que las actuaciones practicadas por esta Agencia han puesto de manifiesto que en su aplicación se presentan problemas interpretativos y que es necesario precisar el ejercicio de estos derechos en relación con algunos ficheros que presentan características especiales"*, y es así que además de establecer los requisitos generales que tienen que cumplir las solicitudes de ejercicio por parte de los afectados, la atención por el responsable del sistema a los derechos de acceso, rectificación y cancelación, también se establecen normas para el ejercicio de los derechos en ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito y en ficheros con fines de publicidad.

1.1.9. Instrucción 1/1995

Esta Instrucción tiene por objeto, siguiendo la regulación establecida por el artículo 29 de la LOPD relativo a los ficheros de información sobre solvencia patrimonial y crédito, atender a los tratamientos de datos personales llevados a cabo con este propósito, y en particular a los tratamientos de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias. En concreto, contiene normas relativas a la calidad de los datos que son objeto de tratamiento, la notificación de la inclusión en el fichero, el cómputo del plazo de seis años (saldo cero), y la adopción de medidas de seguridad.

1.1.10. Instrucción 1/2000

Dado que el régimen aplicable al movimiento internacional de datos ha sido uno de los que más dudas ha suscitado por parte de los responsables de sistemas y de los ciudadanos, la Instrucción 1/2000, según se indica expresamente en su introducción, tiene por objeto *"señalar los criterios orientativos seguidos por la Agencia Española de Protección de Datos en relación con aquellos tratamientos que supongan una transferencia internacional de datos, poniendo de manifiesto el procedimiento que, en uso*

de las competencias que la Ley le atribuye, se sigue por la Agencia en cada caso concreto".

Dicha Instrucción, como no podía ser de otra manera, sigue los principios establecidos en los artículos 33 y 34 de la LOPD, sin suponer innovación alguna. Así, se divide en una sección que contiene disposiciones generales, y en particular la definición de transferencia internacional de datos y donde se recuerda la necesidad de que todo tratamiento que vaya a suponer una transferencia internacional de datos cumpla con las disposiciones de la LOPD, y disposiciones que se aplican a transferencias concretas, las cuales pueden clasificarse atendiendo al país de destino y a la finalidad de la transferencia, ya sea una cesión o comunicación o se trate de una prestación de servicios por parte de un encargado del tratamiento.

1.1.11. Real Decreto 428/1993

El Real Decreto 428/1993, que desarrollaba las previsiones contenidas en la derogada Ley Orgánica 15/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (conocida como LORTAD), en cuanto a la Agencia de Protección de Datos, se debe entender vigente en tanto no se oponga lo dispuesto en la LOPD. En concreto, aprueba el Estatuto de la Agencia Española de Protección de Datos, regulando sus funciones, sus órganos y el régimen económico, patrimonial y de personal.

Por último, cabe señalar que este Real Decreto fue modificado por el Real Decreto 156/1996, de 2 de febrero, para designar a la Agencia Española de Protección de Datos como representante español en el Grupo de Protección de Personas previsto en la Directiva 95/46/CE, de 24 de octubre. Se trata del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE que es un organismo de la Unión Europea con carácter consultivo e independiente, del que actualmente el Director de la Agencia Española de Protección de Datos es Vicepresidente.

1.1.12. Resolución de 30 de mayo de 2000

Mediante esta Resolución de la Agencia Española de Protección de Datos (AEPD), que reemplaza a una Resolución anterior, de 22 de junio, se aprueban los modelos normalizados en soporte papel, magnético y telemático a través de los que los responsables de sistemas de datos deberán efectuar las solicitudes de inscripción de creación, modificación o supresión de sistemas de datos de carácter personal en el Registro General de Protección de Datos. En concreto, establece un modelo para sistemas de datos de titularidad pública y otro para sistemas de datos de titularidad privada.

Es importante tomar en cuenta que la AEPD, en virtud del mandato dado a las Administraciones Públicas por el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en cuanto a promover la incorporación de técnicas electrónicas, informáticas y telemáticas en el desarrollo de su actividad y en el ejercicio de sus competencias, permite el envío de notificaciones relativas a sistemas de datos personales a través de Internet, además de generar un soporte magnético en caso de que deseen presentarse directamente al RGPD.

Es necesario señalar que la AEPD, con fecha 23 de noviembre de 2004, ha publicado a través de su sitio web las versiones actualizadas de estos modelos, tanto en soporte papel como del programa informático de ayuda para la generación de notificación, para adecuar los modelos precedentes al cambio que se produjo en su identidad e imagen institucional así como revisar la lista de terceros países que proporcionan un nivel adecuado de protección de datos[58].

[58] Los modelos en papel, junto con sus instrucciones, para la notificación de sistemas de datos personales se encuentran en el sitio web de la AEPD, para sistemas de datos de titularidad privada en https://www.agpd.es/upload/formprivado.pdf y para sistemas de datos de titularidad pública en https://www.agpd.es/upload/formpublico.pdf. Los programas informáticos para la generación de notificaciones también se encuentran disponibles en el sitio web de la AEPD, el relativo a sistemas de datos de titularidad privada en https://www.agpd.es/upload/RGPD/privado.EXE y para sistemas de datos de titularidad pública en https://www.agpd.es/upload/RGPD/publico.EXE.

1.2. ARGENTINA

Las normas de desarrollo de determinados aspectos de la Ley nº 25.326 son las que se indican a continuación:

Cuestión	Desarrollo normativo
Desarrollo reglamentario de la Ley	❑ Decreto Nº 1558/2001.
Sanciones	❑ Disposición de la Dirección Nacional de Protección de Datos Personales Nº 1/03, de 25 de junio de 2003.
Registro Nacional de Protección de Datos Personales	❑ Disposición de la Dirección Nacional de Protección de Datos Personales Nº 2/03, de 20 de noviembre de 2003.
Censo Nacional de archivos, registros, bases o bancos de datos privados	❑ Disposición de la Dirección Nacional de Protección de Datos Personales Nº 1/04, de 24 de febrero de 2004. ❑ Disposición de la Dirección Nacional de Protección de Datos Personales Nº 3/04.

A continuación reseñamos los aspectos más importantes de las normas indicadas en esta tabla.

1.2.1. Decreto Nº 1558/2001

Este Decreto reglamenta determinados aspectos de la Ley Nº 25.326, en particular lo relativo a los principios generales relativos a la protección de datos, los derechos de los titulares de los datos, los usuarios y responsables de archivos, registros de datos, así como el control de las disposiciones de la Ley y las sanciones aplicables.

1.2.2. Disposición DNPDP Nº 1/03

En virtud de esta Disposición, la Dirección Nacional de Protección de Datos Personales (DNPDP) clasifica las infracciones previstas ante el incumplimiento de la Ley Nº 25.326, en leves, graves y muy graves. También gradúa las correspondientes sanciones. La DNPDP tiene entre sus atribuciones la de imponer las sanciones administrativas por el incumplimiento de la Ley.

1.2.3. Disposición DNPDP Nº 2/03

Crea el Registro Nacional de Bases de Datos, en el que se inscribirán tanto las bases de datos privadas como públicas. Además, aprueba las bases técnico jurídicas del Formulario de Inscripción al Registro Nacional de Bases de Datos y dispone la realización del Primer Censo Nacional de Bases de Datos.

1.2.4. Disposición DNPDP Nº 1/04

Dispone la creación, entre el 1 de marzo y hasta el 30 de abril de 2004, del primer Censo Nacional de archivos, registros, bases o bancos de datos privados, y aprueba el formulario para su notificación telemática. Este plazo fue prorrogado hasta el 30 de junio de 2004 por la Disposición DNPDP Nº 3/04.

1.3. CANADÁ

Cuestión	Desarrollo normativo
Protección de datos en el sector público	❑ Privacy Act (entró en vigor el 1 de julio de 1983).
Protección de datos en el sector privado	❑ Personal Information Protection and Electronic Documents Act (entró en vigor completamemnte el 1 de enero de 2004).

Además de esta legislación a nivel federal sobre la protección de datos personales, que se aplica en el sector público y en el sector privado, casi todas las provincias cuentan con normas similares en protección de datos. Por tanto, es importante tener en consideración que Canadá tiene una compleja regulación sobre la protección de datos, basada en dos normas federales, habiendo entrado en vigor la *Personal Information Protection and Electronic Documents Act* (PIPEDA), que hemos analizado en nuestro Informe por ser la que la Comisión Europea ha examinado para declarar el nivel adecuado de Canadá, en tres fases, completándose el pasado 1 de enero de 2004.

1.4. UNIÓN EUROPEA

En el caso de la Unión Europea por lo que se refiere a la normativa general sobre protección de datos, entendemos necesario prestar atención a las normas que se indican en la siguiente tabla, por regular determinados aspectos que tienen que cumplirse en el tratamiento de datos personales por las instituciones comunitarias así como establecer un órgano supervisor del cumplimiento de esta normativa.

Cuestión	Desarrollo normativo
Terceros países que proporcionan un nivel adecuado a efectos de transferencias internacionales de datos[59] (art. 25)	❑ Decisión 2000/518/CE de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza, publicada en el Diario Oficial L núm. 215, de 25 de agosto. ❑ Decisión 2000/519/CE de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Hungría, publicada en el Diario Oficial L núm. 215, de 25 de agosto[60]. ❑ Decisión 2000/520/CE de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, publicada en el Diario Oficial L núm. 215, de 25 de agosto[61]. ❑ Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic*

[59] Si bien aquí únicamente citaremos las Decisiones aprobadas hasta el momento por la Comisión Europea, ya que todas ellas determinan que los países a que se refieren cumplen con un nivel adecuado de protección de datos de manera que podrá realizarse transferencias con destino a estos países de manera automática, es decir, sin necesidad de autorización previa de la Autoridad de Protección de Datos correspondiente, en los términos previstos en las mismas.

[60] Es necesario tomar en cuenta que Hungría ya es un Estado miembro de la Unión Europea.

[61] Nótese que no se declara que Estados Unidos proporcione un nivel adecuado de protección de datos, sino las entidades que decidan voluntariamente adherirse al Acuerdo de Puerto Seguro. Además, debe atenderse a la corrección de errores de la Decisión 2000/520/CE de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, publicada en el Diario Oficial L núm. 115, de 25 de abril de 2001.

	Documents Act, publicada en el Diario Oficial L 2, de 4 de enero. ❑ Decisión 2003/490/CE de la Comisión, de 30 de junio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina, publicada en el Diario Oficial L núm. 168, de 5 de julio. ❑ Decisión 2003/821/CE de la Comisión, de 21 de noviembre, relativa al carácter adecuado de la protección de los datos personales en Guernsey, publicada en el Diario Oficial L núm. 308, de 25 de noviembre. ❑ Decisión 2004/411/CE de la Comisión, de 28 de abril, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man, publicada en el Diario Oficial L núm. 151, de 30 de abril[62].
Otras entidades (art. 25)	❑ Decisión 2004/496/CE del Consejo, de 17 de mayo, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos, publicada en el Diario Oficial L núm. 183, de 20 de mayo.
Cláusulas contractuales tipo para la transferencia internacional de datos (art. 26)	❑ Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, publicada en el Diario Oficial L núm. 181, de 4 de julio. ❑ Decisión 2002/16/CE de la Comisión, de 27 de diciembre, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE, publicada en el Diario Oficial L núm. 6, de 10 de enero[63].
Tratamiento de datos personales por las instituciones y organismos comunitarios	❑ Reglamento (CE) Nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, publicado en el Diario Oficial L núm. 8, de 12 de enero. ❑ Decisión 2004/644/CE del Consejo, de 13 de septiembre, por la que se adoptan las normas de desarrollo del Reglamento (CE) n° 45/2001 del Parlamento Europeo y

[62] Publicada corrección de errores en el Diario Oficial L 208, de 10 de junio de 2004.

[63] Corrección de errores de la Decisión 2002/16/CE de la Comisión, de 27 de diciembre, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE, publicada en el Diario Oficial L núm. 315, de 19 de noviembre de 2002.

	del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, publicada en el Diario Oficial L núm. 296, de 21 de septiembre.
Supervisor Europeo de Protección de Datos *(European Data Protection Supervisor)*	❑ Decisión nº 1247/2002/CE del Parlamento Europeo, del Consejo y de la Comisión, de 1 de julio, relativa al estatuto y a las condiciones generales de ejercicio de las funciones de Supervisor Europeo de Protección de Datos, publicada en el Diario Oficial L núm. 183, de 12 de julio. ❑ Decisión 2004/55/CE del Parlamento Europeo y del Consejo, de 22 de diciembre, por la que se nombra a la autoridad de vigilancia independiente prevista por el artículo 286 del Tratado CE (Supervisor Europeo de Protección de Datos), publicada en el Diario Oficial L núm. 12, de 17 de enero.

Como hemos señalado anteriormente, únicamente referenciamos las normas generales que, en la Unión Europea, se refieren a la protección de datos de carácter personal, dejando a un lado otras normas sobre aspectos concretos tales como la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 31 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

1.4.1. Reglamento (CE) Nº 45/2001

Este Reglamento establece los principios y obligaciones que tienen que cumplirse en el tratamiento de datos personales por parte de las instituciones y organismos comunitarios, indicando en su Considerando 2º que un sistema completo de protección de datos requiere que se establezcan derechos de las personas, las obligaciones de quienes tratan datos personales, que se prevean sanciones apropiadas para casos de incumplimiento y que se establezca un organismo supervisor independiente (Supervisor Europeo de Protección de Datos).

1.4.2. Decisión 2004/644/CE

Esta Decisión desarrolla el Reglamento (CE) Nº 45/2001 en cuanto a su aplicación por el Consejo de la Unión Europea, determinando el responsable del protección de datos en dicha institución, y el necesario cumplimiento de los principios sobre protección de datos en los tratamientos que se lleven a cabo, los derechos de la protección de datos y el procedimiento para su ejercicio por los interesados, así como el procedimiento de investigación para casos de incumplimiento de la normativa por el responsable del sistema de datos personales.

1.4.3. Decisión nº 1447/2002/CE

Esta Decisión tiene por objeto establecer el procedimiento para la designación del Supervisor Europeo de Protección de Datos y de su Supervisor Adjunto, establecer su sede en Bruselas y determinar algunos criterios, en concreto su asimilación a los jueces del Tribunal de Justicia de las Comunidades Europeas y al Secretario del Tribunal de Justicia de las Comunidades Europeas respectivamente, para su retribución económica.

1.4.4. Decisión 2004/55/CE

Nombra, respectivamente, al Supervisor Europeo de Protección de Datos y a su Supervisor Adjunto, a partir de la propuesta de la lista de candidatos que fue establecida por la Comisión el 22 de abril de 2003, que se elaboró tras la convocatoria pública para la presentación de candidaturas.

2. Inconvenientes e impacto de las legislaciones

A continuación, por cada uno de los ámbitos en los que hemos analizado la correspondiente normativa sobre protección de datos, vamos a atender a los inconvenientes o, mejor dicho, al impacto gubernamental y social que ha tenido la implantación de esta normativa sobre protección de datos, con el propósito de que el IFAI pueda conocer algunos aspectos que deben tomarse en cuenta a la hora de desarrollar una regulación sobre esta materia.

2.1. ESPAÑA

Cuestión	Explicación
Creación de sistemas de datos de carácter personal de titularidad pública y cesión o comunicación de datos entre Administraciones Públicas (arts. 21 y 24).	❑ Recurso de inconstitucionalidad número 1463/2000, promovido por el Defensor del Pueblo, contra determinados preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicado en el Boletín Oficial del Estado número 85, de 8 de abril. ❑ Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica. Publicada en Suplemento al Boletín Oficial del Estado número 4, de 4 de enero de 2001.
Medidas de seguridad	❑ Plazos para la aplicación de las medidas de seguridad en sistemas de datos personales de nivel medio y alto.
Derecho de oposición.	❑ Enunciado en la Ley y no desarrollado.
Censo promocional.	❑ Previsto en la Ley y no desarrollado en la práctica.
Saldo cero.	❑ Mantenimiento de datos adversos relativos a la solvencia patrimonial de la persona durante un plazo máximo de seis años.
Datos relativos a la salud.	❑ Aplicación de las medidas de seguridad de nivel alto en sistemas de datos personales concretos.
Sanciones	❑ Cuantía de las sanciones previstas en la Ley. Aplicación de al previsión contenida en el artículo 45.5 de la LOPD.
Responsable del sistema de datos y encargado del	❑ Determinación de la responsabilidad en casos de incumplimiento del encargado del tratamiento.

tratamiento	"Responsabilidad solidaria".
Transferencia internacional de datos	❑ Sentencia de la Audiencia Nacional de 15 de marzo de 2002, de la Sala de lo Contencioso-administrativo (Sección Primera), por la que se anula parcialmente determinados preceptos de la Instrucción 1/2000 de la Agencia Española de Protección de Datos.
Empresario individual	❑ Protección de los datos personales de las personas que ejercen su actividad como empresarios individuales.
Entrada en vigor de la LOPD.	❑ Alcance de la Disposición Adicional primera en relación con los sistemas de datos personales preexistentes.
Interpretación en el cómputo de los plazos previstos para el ejercicio de los derechos	❑ Días naturales si son sistemas de datos personales de titularidad privada (Código Civil) y días hábiles para sistemas de datos de titularidad pública (Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común).
En general	❑ Necesidad de adecuar la normativa a los cambios introducidos como consecuencia de la transposición de la Directiva 95/46/CE en cuanto a que se tiene que aplicar también a tratamientos no automatizados a partir del 24 de octubre de 2007, sin perjuicio de la atención al ejercicio de los derechos de acceso, rectificación y cancelación por los interesados.
Coordinación entre el Registro General de Protección de Datos de la Agencia Española de Protección de Datos y los Registros de Ficheros de los órganos autonómicos equivalentes.	❑ Firma de un Protocolo de Colaboración para la puesta en marcha del Sistema de Información de Intercambio Registral (SIDIR).
Atribución de competencias sancionadoras	❑ En virtud de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LCE) y de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (LGTel), en cuanto a la imposición de sanciones en supuestos de infracción, lo que ha llevado a plantear si el órgano de control de la normativa sobre protección de datos cuenta con medios, materiales y humanos, suficientes.

De las cuestiones indicadas en la tabla anterior únicamente queremos resaltar algunos aspectos concretos que tienen mayor trascendencia, así por ejemplo la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, ha supuesto la declaración de inconstitucionalidad de los artículos 21.1 y 24.1 y 2, y ha definido el derecho fundamental a la protección de datos, teniendo ello una amplia repercusión en la aplicación de la norma.

En cuanto al derecho de oposición, cabe señalar que se trata de un nuevo derecho, introducido en el ordenamiento jurídico español como consecuencia de la transposición de la Directiva 95/46/CE y que se encuentra solamente referenciado en la LOPD sin que todavía se haya producido su desarrollo reglamentario pero que, sin embargo, el órgano de control ha considerado, conforme a la interpretación de la Directiva 95/46/CE, que le debe ser de aplicación el procedimiento y los plazos previstos para el ejercicio de los derechos de acceso, rectificación y cancelación.

Además, se plantean otras cuestiones que inciden en la interpretación de diferentes aspectos de la LOPD, tal como la extensión de la protección conferida por la Ley a los empresarios individuales cuando no actúen en el tráfico mercantil, dado que la LOPD excluye a las personas morales; el saldo cero, que supone el mantenimiento de datos adversos por un plazo de seis años o la determinación de la responsabilidad entre el responsable del sistema de datos y el encargado del tratamiento, cuando este último comete alguna infracción, en atención a lo elevado de las multas establecidas por la LOPD que llegan a superar los 600.000 euros.

Por último, queremos tomar también en consideración algunas referencias extraídas de la Memoria anual que la Agencia Española de Protección de Datos (AEPD) remite al Ministerio de Justicia, y que permite conocer la doctrina del órgano encargado de velar por el cumplimiento de la normativa sobre protección de datos en diversos aspectos. En este sentido, de la Memoria correspondiente al año 2002[64], cabe destacar que la AEPD pone de manifiesto el incremento de sus actuaciones como consecuencia de la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, citada anteriormente, siendo además esta Memoria uno de los medios que la AEPD tiene para dar a conocer a los ciudadanos y responsables de tratamientos su actividad, con independencia de la presencia que ésta tiene a través de Internet (www.agpd.es) donde los ciudadanos y los responsables de sistemas pueden acceder a una gran cantidad de información sobre la materia.

[64] Disponible en https://www.agpd.es/upload/MemoriaApd2002.pdf.

2.2. ARGENTINA

Respecto de Argentina, cabe señalar que desde la promulgación de la Ley nº 25.326 el 30 de octubre de 2000 han pasado casi de cuatro años hasta que el Director Nacional de Protección de Datos Personales, en ejercicio de las funciones que tiene asignadas, ha procedido a crear el primer Censo Nacional de archivos, registros, bases o bancos de datos privados, lo que da buena muestra de la lentitud con la que se está llevando a cabo la implantación de la normativa sobre protección de datos.

En este sentido, y a pesar de que la Comisión Europea ha reconocido el nivel adecuado de Argentina, es patente que la aplicación de la normativa está casi paralizada, debiendo destacar que la Dirección Nacional de Protección de Datos Personales (DNPDP), que es el órgano de control, tiene una presencia limitada a través de su dirección en Internet (http://www.jus.gov.ar/dnpdp/index.html), en la que no está disponible toda la normativa lo que dificulta en gran medida la posibilidad de analizar su situación actual, sin que tampoco su presencia en Internet se haya mantenido en el tiempo desde su creación.

Aunado a lo anterior, en el Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina (WP 63), adoptado el 3 de octubre de 2002, la Comisión Europea destaca como un punto débil el hecho de que el Director de la Dirección Nacional de Protección de Datos Personales es designado y puede ser destituido por el Ministerio de Justicia y Derechos Humanos, lo que puede plantear dudas acerca de la plena independencia con la que tiene que actuar dicho organismo, instándole a que adoptará las medidas necesarias para subsanar esta situación. Además, la Comisión reconoce en su Dictamen que el análisis del nivel adecuado se basó en los supuestos y explicaciones dadas por el Gobierno argentino y *"no en una experiencia sólida en la aplicación práctica de la legislación, ni a nivel federal ni provincial"*[65].

[65] Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina, página 17. Disponible en http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp63_es.pdf.

En definitiva, cabe concluir que la aplicación de la normativa sobre protección de datos en Argentina resulta deficiente en su aplicación práctica, a pesar de los importantes esfuerzos realizados para estar presente en diferentes foros y participar en actividades a nivel internacional y también a nivel federal.

2.3. CANADÁ

Conforme al último Informe anual de la Autoridad de Protección de Datos canadiense[66], ésta ha trabajado en promover la protección de la privacidad de los ciudadanos, a través de diferentes acciones tales como la culminación de la entrada en vigor de su Ley (PIPEDA) ayudando al sector privado a cumplir con las obligaciones y concienciando a los ciudadanos sobre su derecho a la privacidad. Además, ha respondido cientos de consultas sobre la aplicación de la Ley, y ha llevado a cabo otras actividades dirigidas a la aplicación de la Ley en ámbitos específicos, tales como la salud o las nuevas tecnologías.

Por último, cabe destacar que la autoridad de control ha continuado trabajando en garantizar y mejorar la aplicación de la normativa sobre protección de datos promoviendo, entre otras acciones, la reforma de la *Privacy Act* con el propósito de que el Gobierno de Canadá proteja adecuadamente el derecho a la privacidad de los ciudadanos mediante su adecuación a la nuevas tecnologías; en cuanto a la protección de la privacidad también propone la revisión de la *Anti-terrorism Act*; así como examinar los movimientos internacionales de datos y su impacto en el derecho a la privacidad de los canadienses y adecuar la normativa al avance de las Tecnologías de la Información y las Comunicaciones (TIC), para identificar los riesgos que éstas puedan presentar para la privacidad, en lo que trabajará conjuntamente con órganos federales.

[66] Annual Report for the Office of the Privacy Commissioner of Canada, for the period from April 1, 2003 to March 31, 2004 for the *Privacy Act* and from January 1 to December 31, 2003 for the *Personal Information Protection and Electronic Documents Act*.

2.4. UNIÓN EUROPEA

Tal y como indicábamos al comienzo de este Anexo, para conocer el impacto gubernamental y social que ha tenido la normativa sobre protección de datos, y en particular la Directiva 95/46/CE, en el ámbito de la Unión Europea, es necesario prestar atención al primer informe de la Comisión Europea[67], al informe del Parlamento Europeo sobre este informe[68] y a los resultados de las diferentes consultas y encuestas llevadas a cabo por la Comisión como consecuencia de la aplicación de la Directiva 95/46/CE[69].

De cada uno de los documentos indicados así como de los resultados de las consultas llevadas a cabo por la Comisión, vamos a extraer algunos puntos fundamentales que permitan al IFAI conocer el impacto que esta normativa ha tenido a nivel europeo, remitiéndonos al texto íntegro de los documentos en caso de que se deseen consultar cuestiones concretas y con el propósito de no extendernos en exceso en nuestra exposición.

2.4.1 Informe de la Comisión Europea

En este primer Informe sobre la aplicación de la Directiva 95/46/CE, elaborado con base en la obligación establecida en su artículo 33 de que la Comisión presente al Consejo y al Parlamento Europeo en el plazo de tres años un informe sobre su aplicación y que se acompañe, en su caso, de las oportunas propuestas de modificación, la Comisión ha llevado a cabo un análisis desde una perspectiva amplia, no limitándose únicamente a la aplicación nacional de las leyes sobre protección de datos sino que también ha realizado consultas públicas con el propósito de conocer en mayor medida las implicaciones que ha tenido la aplicación de esta norma.

---

[67] Como ya hemos indicado en una nota anterior, disponible en http://europa.eu.int/eur-lex/es/com/rpt/2003/com2003_0265es01.pdf.

[68] Disponible en http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//NONSGML+REPORT+A5-2004-0104+0+DOC+PDF+V0//ES&L=ES&LEVEL=3&NAV=S&LSTDOC=Y.

[69] Estando disponible esta información en la siguiente dirección de Internet http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm.

Así, entre las conclusiones que se han alcanzado, cabe destacar en primer lugar que la Directiva 95/46/CE no será modificada a corto plazo, dado que la experiencia en su aplicación por los Estados miembros todavía resulta limitada, debido en ello en gran parte a los retrasos en su transposición, y que muchas de las cuestiones que se plantean pueden solventarse sin necesidad de reformar el articulado de la Directiva. Además, en respuesta a las solicitudes de reducir las obligaciones de los responsables de los tratamientos, la Comisión se muestra contraria ya que ello supondría disminuir el nivel de protección de los ciudadanos en cuanto a su derecho fundamental a la privacidad.

Señala también los problemas que puede conllevar la diferencia entre las legislaciones nacionales que transponen la Directiva 95/46/CE, ya que la heterogeneidad puede ser un obstáculo para garantizar la libre circulación de datos en el mercado interior y presentar divergencias en el nivel de protección para los ciudadanos. Lo anterior tiene también consecuencias en la consecución de un sistema normativo flexible y simplificado, lo que determina la necesidad de seguir trabajando para lograr un elevado grado de protección y en la homogenización de la aplicación de la Directiva 95/46/CE en los Estados miembros, incluidos aquellos Estados que se incorporaron a la Unión Europea el 1 de mayo de 2004[70].

2.4.2. Informe del Parlamento Europeo

En el *"Informe sobre el primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)"* (A5-0104-2004 final), de fecha 24 de febrero de 2004, elaborado por la Comisión de Libertades y Derechos de los Ciudadanos, de Justicia y de Asuntos Interiores, el Parlamento Europeo se pronuncia sobre diferentes aspectos de la aplicación de la Directiva 95/46/CE.

[70] En esta fecha se incorporaron a la Unión Europea: Chipre, la República Checa, Estonia, Hungría, Letonia, Lituania, Malta, Polonia, la República Eslovaca y Eslovenia.

En concreto, el Parlamento critica el retraso de la Comisión sobre el establecimiento de un régimen europeo general e interpilares[71] de protección de la privacidad, dado que el derecho fundamental a la protección de datos también tiene que garantizarse en el tercer pilar. Sobre la aplicación de la Directiva 95/46/CE, y dado que el proceso ha sido muy lento por parte de algunos Estados miembros, muestra su acuerdo con la Comisión en que no se lleve a cabo una modificación a corto plazo. También se muestra favorable a la intención de la Comisión de simplificar el régimen para las transferencias internacionales de datos.

Además, en el Informe se contiene la opinión de la Comisión de Asuntos Jurídicos y Mercado Interior, que coincide con la Comisión en que la Directiva 95/46/CE ha cumplido con el objetivo de eliminar algunos de los obstáculos existentes a la libre circulación de datos en el mercado interior y garantizar un elevado grado de protección de la privacidad, además de que resulta prematura una reforma de la norma tomando en cuenta que la aplicación práctica por los Estados miembros es todavía muy limitada.

En definitiva, sin perjuicio de los logros alcanzados, insiste en la tardía transposición de la Directiva 95/46/CE por los Estados miembros e insta a la Comisión a que trabaje en la armonización de esta norma con otras normas que inciden en la privacidad de los ciudadanos europeos.

Por su parte, la Comisión de Industria, Comercio Exterior, Investigación y Energía incide en los obstáculos que puede plantear para el desarrollo del mercado interior la heterogeneidad de las legislaciones nacionales sobre protección de datos e insta a la Comisión a que trabaje de manera conjunta con los Estados miembros para facilitar su aplicación. Por último, señala la importancia de trabajar en la garantía de un elevado nivel de protección de datos y reforzar la aplicación de los principios consagrados en las directrices de la OCDE y del Convenio 108 del Consejo de Europa.

[71] El modelo de estructura de la Unión Europea se basa en tres pilares: primer pilar, las Comunidades Europeas; segundo pilar, la política exterior y de seguridad común, y tercer pilar, cooperación en materia de seguridad interior y política judicial.

2.4.3. Resultados de las consultas y encuestas llevadas a cabo por la Comisión

Tal y como indicábamos anteriormente, la revisión de la aplicación de la Directiva 95/46/CE por parte de la Comisión no se limitó a la transposición llevada a cabo por los Estados miembros, sino que tuvo también en consideración el impacto social de su aplicación, para lo que llevó a cabo un amplio proceso de consultas y encuestas entre diferentes actores interesados (Gobiernos, autoridades de control, empresas y ciudadanos), tanto en línea *(on line)* como por otros medios no electrónicos.

Respecto de esta consulta en línea[72], llevada a cabo el 25 de junio de 2002 con el propósito de conocer la opinión de los ciudadanos y de los responsables de tratamiento sobre la aplicación de la Directiva 95/46/CE, cabe señalar que respondieron un total de 9.156 ciudadanos y 982 responsables de sistemas de datos. En cuanto a las respuestas y las conclusiones que de ellas se obtienen, los datos manejados por la Comisión respecto de algunas cuestiones son que el 44,9% de los ciudadanos considera que el nivel de protección es mínimo, pese a que la Directiva establece normas para conseguir un elevado nivel de protección.

En este mismo sentido, el 81% de los ciudadanos considera que el grado de sensibilización sobre la protección de datos resulta deficiente, frente al 10,3% que lo considera suficiente y al 3,46% que lo considera bueno o muy bueno. Por parte de los responsables de sistemas de datos, también el 30% considera que el grado de sensibilización de los ciudadanos es insuficiente.

En cuanto al cumplimiento de las obligaciones establecidas por la normativa vigente, el 69,1% de los responsables de tratamiento considera que su aplicación es necesaria y sólo un 2,64% estima que los requisitos sobre protección de datos son innecesarios y por tanto que deberían suprimirse.

[72] El cuestionario y los resultados de esta consulta, tanto de los ciudadanos como de los responsables de sistema de datos, se encuentran accesibles en la siguiente dirección de Internet: http://europa.eu.int/comm/internal_market/privacy/lawreport/consultation_en.htm.