Directrices para la armonización de la protección de datos en la Comunidad Iberoamericana*

I. Introducción

El documento sobre desarrollos normativos y armonización, elaborado por el Grupo de Trabajo Permanente de Desarrollo Normativo de la Red Iberoamericana de Protección de Datos en la reunión celebrada en Santa Cruz de la Sierra (Bolivia) los días 3 a 5 de mayo de 2006, considera como una de las máximas prioridades en los trabajos de la Red la elaboración de una propuesta de Directrices contribuir a las iniciativas regulatorias de la Protección de Datos que surjan en la Comunidad Iberoamericana.

El establecimiento de un marco armonizado de protección de datos a nivel global ha sido el principal fundamento de la adopción de los distintos instrumentos internacionales actualmente existentes en materia de protección de datos.

Se trata así de garantizar que el desarrollo del comercio a nivel mundial resulte compatible con la protección de los derechos de las personas, especialmente en lo que se refiere a la protección de la información que les concierne.

De este modo, el establecimiento de un marco homogéneo de regulación del derecho a la protección de datos, bien mediante la adopción de instrumentos supranacionales de carácter vinculante, bien mediante la adopción de Leyes nacionales que consagren el contenido esencial de este derecho, garantizará el desarrollo del comercio en la zona, facilitando el intercambio de información entre los distintos operadores ubicados en los Estados Iberoamericanos y de éstos con terceros países, en particular los Estados miembros de la Unión Europea, en condiciones que no se vean restringidas como consecuencia del distinto nivel de protección del derecho fundamental a la protección de datos de carácter personal.

Así, el Preámbulo de la Recomendación del Consejo de la OCDE, relativa a las Directrices que rigen la protección de la intimidad y la circulación transfronteriza de datos de carácter personal, aprobada el 23 de septiembre de 1980, ya reconoce expresamente que "la circulación transfronteriza de datos personales contribuye al desarrollo

*Adoptadas por la Red Iberoamericana de Protección de Datos en el año 2007.

económico y social", pero al propio tiempo recuerda que "la legislación nacional relativa a la protección de la intimidad y de la circulación transfronteriza de datos personales puede obstaculizar tal circulación transfronteriza".

Por este motivo, la Recomendación parte del objetivo esencial de "fomentar la libre circulación de información entre los países miembro y a evitar la creación de obstáculos injustificados al desarrollo de las relaciones económicas y sociales entre los países miembros". Se pretende así que el intercambio transfronterizo de información no pueda verse limitado por la legislación nacional de protección de datos, pero al propio tiempo garantizar la adecuada protección de este derecho fundamental.

Con mayor claridad si cabe, la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, expresa esta idea en los apartados 6 a 9 de su Exposición de Motivos, indicando lo siguiente:

> (6) Considerando, por lo demás, que el fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones en la Comunidad exigen y facilitan la circulación transfronteriza de datos personales;
>
> (7) Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;
>
> (8) Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para

aproximar las legislaciones;
(9) Considerando que, a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad;"

La mayor parte de las Constituciones de los Estados que constituyen la Comunidad Iberoamericana contienen disposiciones que garantizan a la persona el derecho fundamental a la protección de sus datos personales y el "*habeas data*". Estas previsiones se completan además con las resoluciones dimanantes de los Tribunales de Justicia y, en particular de los Tribunales o Cortes Constitucionales.

Se reconoce así, a través del cauce constitucional y jurisprudencial un derecho fundamental de las personas a la protección de sus datos de carácter personal, independiente y autónomo del derecho a la intimidad, consistente en el derecho del individuo a disponer libremente de la información que le concierna.

Teniendo ello en cuenta, es preciso que los poderes públicos adopten las medidas necesarias para garantizar a las personas la salvaguarda del derecho fundamental, como garantía esencial del estado de derecho.

Sin embargo, el reconocimiento del derecho fundamental debería, como se ha señalado, complementarse con el establecimiento de un marco normativo uniforme, que permita garantizar un nivel equivalente de protección de este derecho, a través del reconocimiento normativo de los principios, derechos y deberes que lo configuran. De este modo podrá asegurarse que, encontrándose plenamente garantizado el derecho fundamental, los Estados Iberoamericanos se beneficien del enriquecimiento económico, social y cultural que puede derivarse del libre intercambio transfronterizo de la información que contiene datos de carácter personal.

El presente documento tiene por objeto delimitar esos perfiles esenciales que configuran el derecho fundamental a la protección de datos de carácter personal, con el

objeto de ofrecer a los poderes públicos de los Estados Iberoamericanos unos criterios orientativos que puedan resultar de utilidad en el desarrollo de las iniciativas normativas que puedan adoptarse, facilitando así el establecimiento de un marco homogéneo de protección que facilite el intercambio de los flujos de información entre todos ellos y desde y hacia terceros Estados que han adoptado estándares similares de protección.

2. El contenido esencial del derecho a la protección de datos personales. Criterios de armonización.

Como ya se ha señalado, la mayor parte de los derechos de los Estados Iberoamericanos reconocen, bien por referencia directa de su Constitución, bien como consecuencia de las decisiones adoptadas por sus órganos judiciales, el derecho de la persona a la protección de datos de carácter personal, esencialmente mediante el reconocimiento del recurso al "*habeas data*", mediante el cual el individuo podrá tomar conocimiento de los datos referidos al mismo y de la finalidad para la que están siendo tratados por un determinado responsable del tratamiento, pudiendo en su caso instar su rectificación, cancelación o actualización.

El ejercicio de este derecho ha dado lugar a una rica jurisprudencia que ha evolucionado hacia el reconocimiento de una serie de principios a los que deben someterse las Administraciones Públicas y las entidades privadas que tratan datos de carácter personal.

En Colombia, la Corte Constitucional a través de más de 140 sentencias ha definido el alcance y características del habeas data así como las condiciones que deben rodear el tratamiento de los datos personales consagrado en el artículo 15 de la Constitución de 1991.

Desde la primera sentencia (T 414/92) la Corte ha establecido que la persona es el titular y propietario del dato personal. Para ella es obligación de los administradores de bancos de datos administrar correctamente y proteger los archivos y bases de datos que contengan información personal o socialmente relevante y no atentar contra los derechos fundamentales de las personas. La Corte Constitucional señaló, de manera general, que "*la función de administrar una base de datos debe fundamentarse en los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad*". Concretamente, ha precisado que los administradores deben: (1) Obtener previamente la autorización de la persona cuyos datos se pretende incluir en la base; (2) Notificar a la persona sobre la inclusión de sus datos en el banco e informarle que va a reportar su información en una base de datos con miras a que el titular pueda desde un comienzo ejercer sus derechos de rectificación y actual-

ización;(3) Actualizar permanente y oficiosamente la información para que ésta sea veraz, completa y no se omitan factores que pueden cambiar el buen nombre de la persona; (4) Eliminar de oficio la información negativa que ha caducado con el paso del tiempo; (5) Indemnizar los perjuicios causados por la falta de diligencia o por posibles fallas en el manejo, tratamiento o administración de datos personales; (6) Garantizar el derecho de acceso, actualización y corrección. Estos derechos implican que la persona tenga "*la posibilidad (...) de saber en forma inmediata y completa, cómo, por qué y dónde aparece cualquier dato relacionado con él"; (...)si la información es errónea o inexacta, el individuo puede solicitar, con derecho a respuesta también inmediata, que la entidad responsable del sistema introduzca en él las pertinentes correcciones, aclaraciones o eliminaciones, a fin de preservar sus derechos fundamentales vulnerados*". Finalmente, la Corte ha precisado que, por regla general, "*no puede recolectarse información sobre datos "sensibles" como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación*".

En España, la Sentencia 292/2000, de 30 de noviembre, tras desvincular el derecho a la protección de datos del derecho a la intimidad, señala que "*el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso*", añadiendo que "*estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero*". Así, se concluye que "*son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele*".

En México, el derecho a la protección de datos personales se aplica en el ámbito de los ficheros públicos a nivel federal en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LAI), y cada legislatura estatal, en el marco de sus leyes de acceso a la información, incluyen capítulos ad-hoc.

Actualmente, existen dos iniciativas de reforma constitucional, la primera presentada

ante la Cámara de Senadores que adiciona el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos para reconocer al derecho a la protección de datos personales, como un derecho fundamental, mismo que fue aprobado en la anterior legislatura y fue enviado a la Cámara de Diputados para los efectos constitucionales correspondientes, estando aún pendiente su discusión y aprobación en ésta última. La segunda iniciativa se presentó el pasado 27 de marzo de 2007 de abril, que vendría a reforzar la señalada anteriormente, ya que dota al Congreso de facultades expresas para expedir la ley de la materia, esgrimiendo que es relevante no sólo por tratarse de un tema de protección de derechos humanos y libertades fundamentales, sino por los efectos esenciales que estos tienen sobre la economía nacional. *Finalmente, es de señalar que el Pleno del IFAI, en su sesión del 25 de abril de 2007, aprobó por unanimidad* que se conforme un grupo de trabajo entre el sector privado y dicho instituto, para la elaboración de un borrador de proyecto de Ley en materia de Protección de Datos Personales.

En el Perú diversa jurisprudencia del Tribunal Constitucional se ha pronunciado sobre el reconocimiento del derecho a la autodeterminación informativa que reconoce el artículo 2°, inciso 6) de la Constitución Política de 1993 y, asimismo ha señalado el objeto de este derecho, su naturaleza relacional y marcado las diferencias entre éste y otros derechos humanos como los de la intimidad, imagen e identidad personal.

Así por ejemplo, la sentencia de fecha 29 de enero recaída en el Exp. N° 1797- 2002-HD/TC, señala que *"El derecho reconocido en el inciso 6) del artículo 2° de la Constitución es denominado por la doctrina derecho a la autodeterminación informativa y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución (...) por su propia naturaleza, el derecho a la autodeterminación informativa, siendo un derecho subjetivo tiene la característica de ser, prima facie y de modo general, un derecho de naturaleza relacional, pues las exigencias que demandan su respeto, se encuentran* muchas veces vinculadas a la protección de otros derechos constitucionales." La sentencia citada ratifica lo expresado en la sentencia recaída en el Exp. N°. 666-1996-HD/TC , precisando lo que incluye la protección del derecho a la autodeterminación informativa a través del hábeas data, señalando que comprende: *"en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información así como la (o las) persona(s) que recabaron dicha información. En segundo lugar, el hábeas data puede tener la*

finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo, con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados.".

Por su parte, en Europa, el derecho fundamental a la protección de datos de carácter personal ha sido expresamente reconocido como derecho fundamental y claramente diferenciado del derecho a la intimidad personal y familiar de las personas por el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, cuyo artículo 8 establece lo siguiente:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Los apartados 2 y 3 de este precepto delimitan el contenido esencial que debe revestir la legislación que regule el derecho fundamental a la protección de datos de carácter personal. De este modo:

-Los datos deberán ser tratados de modo leal.

-Los datos deberán ser tratados para fines concretos.

-El tratamiento deberá efectuarse sobre la base del consentimiento del interesado o como consecuencia de algún otro fundamento legítimo y previsto legalmente.

-Toda persona tendrá los derechos de acceso, rectificación y cancelación al tratamiento.

-Deberá existir una autoridad independiente encargada de velar por la garantía del derecho.

Por otra parte, distintos instrumentos internacionales, procedentes de Organismos Supranacionales de los que son miembros todos o parte de los Estados Iberoamericanos han venido a establecer los principios básicos que configuran el derecho a la protección de datos personales.

Así, la ya citada recomendación de la OCDE delimita estos principios, enumerando como básicos los siguientes.

1. Aplicación a todo tratamiento de datos del sector público y del privado
2. Interpretación restrictiva de las posibles exclusiones a la aplicación de los principios
3. Principio de limitación de la recogida
4. Principio de calidad de los datos
5. Principio de especificación de la finalidad
6. Principio de limitación de uso
7. Principio de salvaguardas de seguridad
8. Principio de apertura
9. Principio de participación individual (Habeas data)
10. Principio de responsabilidad
11. Garantías de la circulación transfronteriza, ininterrumpida y segura, de los datos personales, entre los Estados que observen los principios
12. Establecimiento de sanciones y recursos suficientes en caso de incumplimiento.

A su vez, deben tenerse en cuenta las Directrices para la regulación de los archivos de datos personales informatizados, adoptadas mediante Resolución 45/95 de la Asamblea General de las naciones Unidas, de 14 de diciembre de 1990, que consideran como garantías mínimas que deben prever las legislaciones nacionales los siguientes principios:

1. Principio de legalidad y lealtad
2. Principio de exactitud
3. Principio de especificación de la finalidad
4. Principio de acceso de la persona interesada
5. Principio de no discriminación
6. Limitación de la facultad para hacer excepciones
7. Principio de seguridad
8. Supervisión y sanciones, a través de una autoridad que deberá ofrecer garantías de imparcialidad, independencia y competencia técnica 9. Flujo transfronterizo de datos basado en la similitud de las salvaguardas10. Campo mínimo de aplicación general a todos los archivos informatizados públicos y privados.

Junto con estos instrumentos, no debe olvidarse el análisis producido en el ámbito de la Unión Europea en cumplimiento de la Directiva 95/46/CE. La importancia de la Directiva en el ámbito supraeuropeo resulta esencial, en primer lugar, dado que se trata del texto internacional que regula con mayor precisión y detalle los principios, derechos

y deberes que configuran el derecho fundamental a la protección de datos.

Además, debe recordarse que el fundamento de la Directiva, como ya se ha indicado consiste en establecer un marco armonizado de protección del derecho a la protección de datos personales que garantice el libre flujo de información en el ámbito de la Unión Europea, favoreciendo así el comercio y el enriquecimiento derivado de los flujos de información.

Por último, no debe olvidarse que los artículos 25 y 26 de la Directiva establecen un régimen específico para los flujos transfronterizos de datos de carácter personal, exigiendo, como punto de partida, que el Estado al que se destinen los datos ofrezca un nivel adecuado de protección de datos de carácter personal. De este modo, la Directiva da cumplimiento al principio esencial de equilibrio entre la libre transmisión de información y la protección del derecho de las personas.

Por tanto, la asunción de principios que puedan considerarse "adecuados" a los previstos en la Directiva puede constituirse como un punto de partida adecuado para facilitar los flujos transfronterizos de información a ambos lados del Atlántico manteniendo unas adecuadas garantías del derecho fundamental a la protección de datos de carácter personal. No se trata así de obtener una aplicación transfronteriza de la legislación europea, sino de lograr una adecuada conciliación entre ambos.

En el ámbito Iberoamericano, deben citarse los esfuerzos realizados en el ámbito de la UNESCO y la Estrategia Latinoamericana de la Sociedad de la Información (ELAC) llevada a cabo en el seno de la CEPAL, con el objeto de lograr el diseño de mecanismos de armonización normativa en el ámbito de la privacidad y protección de datos personales.

Asimismo, debe señalarse que algunos Estados han adoptado en los últimos años iniciativas en este sentido. Así, no debe olvidarse los desarrollos normativos llevados a cabo por Argentina, que culminaron en la Adopción de la Decisión de la Comisión de 30 de junio de 2003, por la que se considera que dicho Estado garantiza un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad.

En este marco, puede resultar interesante para el análisis la actividad desarrollada por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE; en particular su Dictamen 4/2002, de 3 de octubre, sobre el nivel de protección de datos personales en Argentina.

Los diversos dictámenes aprobados en el seno del mencionado Grupo de Trabajo en relación con el nivel de protección de datos en terceros Estados han tomado como referente el documento de trabajo del Grupo sobre Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, aprobado el 24 de julio de 1998, cuyo Capítulo 1 analiza qué debe entenderse por "protección adecuada".

A tal efecto, el documento delimita dos tipos de análisis que habrían de efectuarse sobre la legislación del Estado de destino de los datos, a fin de poder delimitar si la misma resulta adecuada: el relativo a su contenido sustantivo y el relacionado con los mecanismos y procedimientos de aplicación de la legislación sustantiva.

n cuanto al contenido sustantivo, la legislación del Estado de destino habría de contener los principios básicos de protección de datos que tradicionalmente han venido siendo reconocidos por los acuerdos y directrices internacionales adoptados en este ámbito, y que se han señalado con anterioridad, considerándose como tales los siguientes:

1. Limitación de la finalidad
2. Calidad y proporcionalidad de los datos
3. Transparencia
4. Seguridad y confidencialidad
5. Derechos de acceso, rectificación, supresión y bloqueo de los datos
6. Restricciones a la transferencia ulterior
7. Categorías especiales de datos
8. Marketing directo
9. Decisión individual automatizada

Estos principios, como mínimo, deberían aparecer recogidos en la legislación del Estado destinatario de los datos para que pudiera considerarse que el mismo ofrece un nivel adecuado de protección.

Lógicamente, para que pueda considerarse que existe un efectivo reflejo legal de estos principios en la legislación del Estado en cuestión será preciso que dicha normativa tenga un ámbito general de aplicación a los tratamientos efectuados por los sectores público y privado, de forma que no se establezcan más límites a su aplicación que los relacionados con la actividad meramente personal o familiar de quien los lleva a cabo o sean adecuadas limitaciones al derecho fundamental en el marco de actividad de una sociedad democrática.

Por otra parte, en cuanto al análisis referido a los procedimientos de aplicación de las normas sustantivas, el documento considera que la existencia de los mismos es indispensable para que un sistema de protección de datos pueda, en la práctica, otorgar un nivel adecuado de protección, dado que supone la existencia de mecanismos de control de los principios contenidos en las leyes nacionales.

Tal y como indica el documento este elemento se materializa generalmente en el establecimiento de una autoridad independiente de protección de datos y en la regulación de procedimientos adecuados que permiten a los afectado obtener la protección de sus derechos o la reparación de los perjuicios que les han sido causados.

Así, como regla general, podrá considerarse que el Estado otorga un nivel de protec-

ción adecuado en los supuestos en los que el mismo cuente con una norma reguladora de la protección de datos que contenga los principios sustantivos que se han enumerado y exista una autoridad encargada de velar por su cumplimiento, ante la cual los interesados puedan dirigir sus reclamaciones y que ostente poderes de inspección e investigación de los tratamientos.

Un último requisito esencial de dicha autoridad será su capacidad para imponer medidas que garanticen la efectividad del derecho, tales como sanciones en caso de incumplimiento o, cuando menos, la capacidad para instar a los Tribunales la imposición de esas medidas en los casos en los que del uso de sus poderes de investigación se desprenda que existe una vulneración de la normativa de protección de datos.

El análisis que se ha descrito ha permitido al Grupo dictaminar favorablemente la adecuación del nivel de Protección de Datos personales de los Estados respecto de los que posteriormente se ha adoptado una Decisión en este sentido por parte de la Comisión. Basta con analizar el ya citado Dictamen 4/2002, referido al nivel de protección de datos en Argentina, para comprobar que su estructura y análisis se fundamenta en lo establecido en el citado documento de trabajo.

3. Directrices (principios, derechos y obligaciones) que deberá contener una Ley nacional de protección de datos de carácter personal:

1. Ámbito de aplicación

1.1. Las presentes directrices serán de aplicación a todo tratamiento manual o automatizado de datos de carácter personal, entendiéndose como tales cualquier información referida a personas físicas identificadas o identificables. En consecuencia, las directrices serán aplicables a los tratamientos llevados a cabo por todas las entidades de los sectores público y privado.

1.2. No obstante, será posible excluir de las directrices el tratamiento manual o no automatizado cuando los datos objeto de tratamiento no vayan a ser incorporados a un fichero estructurado con arreglo a criterios que permitan la identificación de las personas cuyos datos son sometidos a tratamiento

1.3. Igualmente, no serán aplicables las directrices al tratamiento de datos de carácter personal, automatizado o manual, que una persona física realice para fines exclusivamente relacionados con su vida privada o familiar.

1.4. Será posible la exclusión de la aplicación de los apartados 2, 3, 4, 5, 6.1, 6.2, 6.3 y 8 de las presentes directrices mediante una Ley nacional de determinados tratamientos

de datos de carácter personal en la medida que la aplicación de las directrices pudiera suponer un riesgo para la protección de la seguridad nacional, el orden público, la salud pública o la moralidad y dicha medida resulte estrictamente necesaria y no excesiva en el ámbito de una sociedad democrática.

2. Principios relacionados con la finalidad y calidad de los datos

2.1. Tratamiento leal y lícito: los datos sólo podrán ser recabados y tratados de buena fe, con estricto respeto por la Ley y los derechos de las personas y de conformidad a lo previsto en las presentes directrices.
2.2. Limitación de la finalidad: los datos únicamente podrán ser recabados y tratados para el cumplimiento de las finalidades determinadas, explícitas y legítimas relacionadas con la actividad de quien los trate.

No podrán ser tratados para fines distintos de aquéllos que motivaron su obtención a menos que exista legitimación suficiente para ello, conforme a lo establecido en el apartado 3 de estas directrices.
2.3. Principio de proporcionalidad: Sólo podrán ser sometidos a tratamiento los datos que resulten adecuados, pertinentes y no excesivos en relación con las finalidades a las que se refiere el punto anterior.
2.4. Principio de exactitud: Los datos deberán mantenerse exactos, completos y puestos al día, respondiendo a la verdadera situación de la persona a la que se refieran.
2.5. Principio de conservación: Los datos deberán ser cancelados o convertidos en anónimos cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades que justificaron su obtención y tratamiento

3. Legitimación para el tratamiento

3.1. Los datos sólo podrán ser recabados o tratados en caso de que se hubiera obtenido el consentimiento del interesado.
3.2. No obstante la Ley podrá establecer supuestos en los que no será necesario el consentimiento del interesado para el tratamiento de sus datos personales, atendiendo a las circunstancias que concurran en cada supuesto y, en todo caso, siempre que dicha excepción no perjudique los derechos fundamentales del interesado. En particular, la Ley podrá permitir el tratamiento de los datos sin contar con el consentimiento del interesado cuando el mismo se realice en el marco de una relación jurídica o por una Administración en el ejercicio de las potestades que le hayan sido atribuidas.

3.3. Los datos que revelen la ideología, afiliación sindical, religión o creencias del afectado sólo podrán ser tratados con su consentimiento, a menos que aquél los hubiera hecho

manifiestamente públicos.
3.4. Los datos relacionados con la salud, el origen racial y la vida sexual del afectado únicamente podrán ser recogidos y tratados en los supuestos mencionados en el párrafo anterior o cuando una Ley así lo disponga.
3.5 En todo caso las presentes directrices no obstaculizarán el adecuado tratamiento médico del interesado ni la atención de una urgencia vital del mismo.

4. Transparencia e información al interesado

4.1 El interesado del que se recaben los datos deberá ser informado al tiempo de su recogida de la identidad del responsable del tratamiento, los fines para los que los datos vayan ser tratados y el modo en que podrá hacer efectivos los derechos a los que se refieren los apartados 5 y 6 de estas directrices, así como de cualquier otra información necesaria para garantizar un tratamiento lícito de los datos. Esta obligación solamente quedará exceptuada si el interesado hubiera sido ya informado con anterioridad de estas circunstancias.
4.2. Cuando los datos no hayan sido obtenidos del interesado deberá informarse al mismo de los extremos previstos en el párrafo anterior en un plazo prudencial de tiempo y, en todo caso, con anterioridad a que los datos sean comunicados a un tercero.

5. Derechos de acceso, rectificación y cancelación de los interesados

El interesado cuyos datos sean objeto de tratamiento podrá, a través de procedimientos claros, expeditos y gratuitos o sin gastos excesivos:
5.1 Recabar del responsable del tratamiento 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.
5.2. Recabar del responsable del tratamiento información, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos.
5.3. Exigir, en su caso, la rectificación o cancelación de los datos que pudieran resultar incompletos, inexactos, inadecuados o excesivos, con arreglo a lo previsto en las presentes directrices.
5.4. Exigir que se notifique a los terceros a quienes se hayan comunicado los datos de toda rectificación o cancelación efectuado conforme al párrafo anterior.

6. Otros derechos de los interesados

Además de los derechos a los que se refiere el apartado anterior, los interesados tendrán los siguientes:

6.1. No verse sometidos a decisiones 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 o conducta. No obstante, será posible la adopción de dichas decisiones cuando se verifiquen en el marco de una relación jurídica libremente aceptada por el interesado, en que se concede al mismo la posibilidad de efectuar alegaciones acerca del resultado de la valoración.

6.2. Oponerse al tratamiento de sus datos, en supuestos no excluidos en virtud de la Ley, como consecuencia de la concurrencia de una razón excepcional y legítima derivada de su concreta situación personal.

6.3. Oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable vaya a llevar a cabo un tratamiento para actividades vinculadas con la publicidad y la prospección comercial.

6.4. Recabar el auxilio de los tribunales y de las autoridades a las que se refiere el apartado 9 de estas directrices en caso de considerar que el tratamiento de sus datos se está llevando a cabo con conculcación de las mismas.

6.5. Ser indemnizados por cualquier daño o lesión que hubieran sufrido en sus bienes o derecho como consecuencia del tratamiento de datos llevado a cabo con conculcación de lo dispuesto en estas directrices.

7. Seguridad y confidencialidad en el tratamiento

7.1. Deberán adoptarse las medidas técnicas y organizativas que resulten necesarias para proteger los datos contra su adulteración, pérdida o destrucción accidental, el acceso no autorizado o su uso fraudulento.

7.2. Quienes 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.

8. Limitaciones a la transferencia internacional de datos

8.1. Como regla general sólo podrán efectuarse transferencias internacionales de datos al territorio de Estados cuya legislación recoja lo dispuesto en las presentes directrices.

8.2. No obstante la Ley podrá establecer supuestos en que, excepcionalmente, sea posible la transferencia internacional de datos a otros Estados, atendiendo a las circunstancias

que concurran en cada supuesto. En todo caso, deberán tenerse en cuenta los derechos e intereses del afectado y, en particular, si el mismo ha prestado su consentimiento a la transferencia en cuestión.

8.3. Fuera de los supuestos mencionados en los dos párrafos anteriores, sólo será posible la transferencia internacional de datos en caso de que se obtenga la autorización de la autoridad a la que se refiere el apartado 9, para lo cual será necesaria la aportación por parte del exportador de garantías suficientes para asegurar que el importador cumplirá en todo caso lo dispuesto en estas directrices.

9. Autoridades de control

9.1. La garantía del cumplimiento de estas directrices deberá quedar sujeto al control de una o varias autoridades de protección de datos. Las autoridades podrán tener personalidad propia o encontrarse integradas en la Administración Pública o en un Organismo Público preexistente. Igualmente podrán tener como función exclusiva el cumplimiento de las normas de protección de datos o ejercer tal competencia junto con otras atribuidas por su legislación.

La organización territorial del Estado no podrá suponer un obstáculo para que las garantías derivadas de la existencia de la o las autoridades de protección de datos sean reales y efectivas en relación con todos los tratamientos llevados a cabo tanto por el sector público como por el privado.

9.2. Las autoridades de protección de datos deberán actuar con plena independencia e imparcialidad, no pudiendo estar sometidas en el ejercicio de sus funciones al mandato de ninguna autoridad pública. Deberán establecerse mecanismos que garanticen la independencia e inamovilidad de las personas a cuyo cargo se encuentre la dirección de dichas autoridades.

9.3 Las autoridades deberá tener como mínimo las siguientes competencias:

-Conocer de las reclamaciones que les sean dirigidas por los interesados, en particular en cuanto al ejercicio de los derechos a los que se refiere el apartado 5 de estas directrices.

-Realizar las averiguaciones e investigaciones que resulten necesarias para el cumplimiento de las directrices, pudiendo acceder a los datos que sean objeto de un tratamiento y recabar toda la información necesaria para el cumplimiento de su misión de control.

-Adoptar las medidas que resulten necesarias para evitar la persistencia en el incumplimiento de las directrices.

-Mantener un registro de los tratamientos llevados a cabo por los sectores público y privado, al que puedan acceder los interesados, a fin de poder ejercer los derechos

reconocidos en las presentes directrices. La solicitud de inscripción se realizará mediante modelos simplificados y basados en estándares técnicos, respetando el principio de neutralidad tecnológica, utilizándose siempre que ello sea posible técnicas o medios electrónicos.
-Autorizar, cuando sea preciso, las transferencias internacionales de datos a Estados cuya legislación no recoja lo dispuesto en las presentes directrices.
-Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales que: (i) represente un valor añadido en su contenido respecto de lo dispuesto en las leyes, (ii) contenga o esté acompañado de elementos que permitan medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales y (iii) consagre medidas efectivas en caso de su incumplimiento.
-Dictaminar los proyectos de disposiciones normativas que puedan afectar al derecho fundamental a la protección de datos personales.
-Divulgar a los individuos y a los poderes públicos el contenido del derecho fundamental a la protección de datos personales.
-Cooperar con las autoridades de protección de datos para el cumplimiento de sus competencias y generar los mecanismos de cooperación bilateral y multilateral para asistirse entre si y prestarse el debido auxilio mutuo cuando se requiera.

10. Sanciones

10.1. El incumplimiento de las disposiciones que reflejen lo previsto en estas directrices deberá ser sancionado conforme a la legislación interna. La capacidad para la imposición de las correspondientes sanciones podrá corresponder a la autoridad de protección de datos, a la que se refiere el apartado 9 o a los órganos judiciales.
10.2 En todo caso, las autoridades de protección de datos deberán tener capacidad suficiente para recurrir a las vías judiciales que resulten competentes para lograr la adopción de las medidas necesarias para garantizar el cumplimiento de estas directrices y, en particular, la imposición de las sanciones que correspondiesen.
10.3. Si las autoridades de protección de datos fueran directamente competentes para la imposición de sanciones, sus resoluciones deberán ser recurribles ante los Tribunales de Justicia.