



**11081/02/ES/Final  
WP 63**

**Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina**

**Adoptado el 3 de octubre de 2002**

El Grupo de Trabajo, creado por el artículo 29 de la Directiva 95/46/CE, es un órgano consultivo independiente de la UE sobre protección de datos y vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

La secretaría está a cargo de: Dirección A (Funcionamiento e Impacto del Mercado Interior, Coordinación y Protección de Datos), Dirección General de Mercado Interior, Comisión Europea, B-1049 Bruselas, Bélgica, Despacho C100-6/136.  
Internet: [www.europa.eu.int/comm/privacy](http://www.europa.eu.int/comm/privacy)

**DICTAMEN DEL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES**  
**creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995**

**sobre el nivel de protección de datos personales en Argentina**

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES,

Vista 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<sup>1</sup>, y, en particular, su artículo 29 y la letra b del apartado 1 de su artículo 30,

Visto su Reglamento interno<sup>2</sup>, y, en particular, sus artículos 12 y 14,

Considerando lo siguiente:

- (1) El Gobierno de la República Argentina solicitó<sup>3</sup> a la Comisión que determinara si Argentina garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el artículo 25 de la Directiva.
- (2) La Comisión Europea solicitó el dictamen del Grupo de Trabajo al respecto.

HA ADOPTADO EL PRESENTE DICTAMEN:

**1. INTRODUCCIÓN: LEGISLACIÓN ARGENTINA SOBRE PROTECCIÓN DE DATOS**

La legislación argentina regula la protección de datos personales mediante diversos instrumentos jurídicos, que pueden clasificarse en normas generales y sectoriales.

**1.1. Normas generales**

Las normas generales resultan de combinar la Constitución, la Ley 25 326 sobre protección de datos personales y el Decreto Reglamentario n° 1558/2001 que, juntos, conforman el régimen jurídico común aplicable a la protección de datos personales.

• ***Constitución argentina***

La Constitución argentina prevé un recurso judicial especial, denominado «*habeas data*», para proteger los datos personales. Se trata de un subtipo del procedimiento

---

<sup>1</sup> DO L 281, 23.11.1995, p. 31, que puede consultarse en:

[http://europa.eu.int/comm/internal\\_market/en/media/dataprot/index.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm).

<sup>2</sup> Adoptado por el Grupo de Trabajo en su tercera reunión celebrada el 11.9.1996.

<sup>3</sup> Carta del Embajador de la República Argentina ante la Unión Europea, de 23 de enero de 2002.

contemplado en la Constitución para proteger los derechos constitucionales y, por tanto, eleva la protección de datos personales a la categoría de derecho fundamental. En particular, el tercer párrafo del artículo 43 de la Constitución argentina establece que «toda persona podrá interponer esta acción (es decir, el *habeas data*) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística».

La jurisprudencia argentina ha reconocido el *habeas data* como un derecho fundamental y directamente aplicable.

- ***Ley sobre protección de datos personales, de 4 de octubre de 2000 (Ley 25 326, en adelante denominada «la Ley»)***

La Ley desarrolla y amplía lo dispuesto en la Constitución. Contiene disposiciones 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 data*.

- ***Decreto Reglamentario n° 1558/2001, de 3 de diciembre de 2001 (en adelante denominado «el Reglamento»)***

Este Reglamento establece las normas de aplicación de la Ley, completa lo dispuesto en ella y clarifica aspectos de la Ley que podrían interpretarse de manera divergente.

Estos tres instrumentos jurídicos constituyen las normas generales de la legislación argentina en materia de protección de datos (en adelante, «la legislación argentina»).

### **Ámbito de aplicación de la legislación argentina**

El Grupo de Trabajo evaluó la adecuación del nivel de protección de datos personales proporcionado en conjunto por la Constitución argentina, la Ley 25 326 y el Decreto Reglamentario n° 1588/2001. Por tanto, el presente dictamen se limita al ámbito de las citadas normas y no es aplicable a situaciones no cubiertas por dichos instrumentos jurídicos. El Grupo de Trabajo ha tenido especialmente en cuenta las explicaciones y garantías proporcionadas por las autoridades argentinas sobre la forma en que debe interpretarse lo dispuesto en la Constitución, la Ley y el Reglamento y sobre las situaciones a las que se aplica la legislación argentina de protección de datos.

### ***Ámbito de aplicación material***

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales la legislación argentina de protección de datos cubre las situaciones siguientes:

- i. *En relación al responsable de la base de datos*

La legislación argentina cubre la protección de:

- 1) *Los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos públicos.* El Grupo de Trabajo interpreta que el responsable de la base de datos es una institución u organismo público. Dicha interpretación se deduce claramente del artículo 43 de la Constitución y del artículo 1 de la Ley;
- 2) *Los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos privados*
  - a) *si los archivos, registros o bancos de datos exceden el uso exclusivamente personal.* El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales todo uso que pueda afectar a los derechos del titular de los datos debe considerarse que excede el uso exclusivamente personal;
  - o
  - b) *incluso si los archivos, registros o bancos de datos no exceden el uso exclusivamente personal, si 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.*

El Grupo de Trabajo interpreta que a) y b) se refieren a situaciones en las que el responsable de la base de datos es una entidad privada, sea persona física o jurídica.

En cuanto a los archivos de datos privados, el Grupo de Trabajo observa que tanto el tercer párrafo del artículo 43 de la Constitución como el artículo 1 de la Ley se refieren a «archivos, registros, bancos de datos u otros medios técnicos privados, destinados a dar informes». La misma redacción aparece en otras disposiciones de la citada Ley, como los artículos 14 (derecho de acceso), 21 (obligación de inscribirse en el Registro), 29 (atribuciones del órgano de control), 33 y 35 (requisitos del recurso judicial *habeas data*) y 46 (disposiciones transitorias). No obstante, la interpretación amplia antes indicada se desprende de varios argumentos expuestos por las autoridades argentinas:

- El artículo 1 del Reglamento proporciona una interpretación jurídica de la Ley. En particular, define jurídicamente el concepto de «archivos, registros, bases o bancos de datos privados destinados a dar informes» como «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».
- El artículo 24 de la Ley dispone que «los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21». El artículo 21 de la Ley obliga a inscribir en el Registro las bases de datos privadas *destinadas a proporcionar informes*. El artículo 24 no tendría sentido si la Ley sólo se aplicara a las bases de datos destinadas a proporcionar informes. Estos dos artículos confirman el paralelismo de las expresiones «bases de datos *destinadas a proporcionar informes*» y «bases de datos [...] *que no sean para un uso*

*exclusivamente personal*», como establece la definición jurídica del artículo 1 del Reglamento (véase el primer argumento citado anteriormente).

- Por otra parte, cabe mencionar que tanto la Ley como el Reglamento contienen normas sobre tratamiento de datos relativos a la salud (artículo 8 de la Ley) o publicidad directa (artículos 27 de la Ley y el Reglamento), según las cuales dichas bases de datos, aunque exceden el uso exclusivamente personal, no pueden estar destinadas a proporcionar informes. Una vez más, estas normas serían superfluas si la Ley sólo fuera aplicable a las bases de datos destinadas a proporcionar informes.

Según las autoridades argentinas, los tribunales de dicho país han seguido la interpretación amplia mencionada anteriormente<sup>4</sup>.

*ii. En relación al titular de los datos*

En relación con el tratamiento de datos personales, la legislación argentina protege tanto a las personas físicas como a las personas jurídicas. El artículo 2 de la Ley define «titular de los datos» como «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», y el artículo 1 de la Ley establece que «las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal». El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales el requisito de disponer de domicilio legal, delegaciones o sucursales en Argentina sólo es aplicable a las personas jurídicas titulares de datos y no a las personas físicas. Por tanto, todas las personas físicas son titulares de datos y están protegidas por la legislación argentina.

*iii. En relación al método de tratamiento*

La legislación argentina abarca la protección de datos personales tanto si su tratamiento es manual como automático. En particular, el artículo 2 de la Ley define «tratamiento de datos» como «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».

*iv. En relación a la finalidad de las operaciones de tratamiento*

El Grupo de Trabajo observa que la legislación argentina tiene al respecto un ámbito de aplicación general. Ya que ninguna norma define la finalidad de las bases de datos sujetas a la legislación, el Grupo de Trabajo interpreta que ésta se aplica en principio a todos los archivos, registros y bancos de datos sea cual sea su finalidad, salvo si se dispone lo contrario. Sin embargo, el Grupo de Trabajo señala los siguientes aspectos:

- Tratamiento de datos con fines de defensa nacional, seguridad pública o represión de delitos

---

<sup>4</sup> Cámara Civil de Apelación, Mantovano c/ Banco Regional de Cuyo, 2000; Becker José c/ Banco de la provincia de Buenos Aires, 2002

Estas operaciones están sujetas a la Ley. En dichos supuestos se aplican las normas generales de la Ley y el Reglamento, sin perjuicio de lo dispuesto expresamente en el artículo 23 de la Ley como *lex specialis*, que confirma el principio de limitación de la finalidad.

– Tratamiento de datos con fines periodísticos

El párrafo 3 del artículo 43 de la Constitución dispone que «no podrá afectarse el secreto de las fuentes de información periodística». En la misma línea, el artículo 1 de la Ley afirma que «en ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas».

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales esta norma tiene como objetivo proteger el secreto de las fuentes de información periodística como condición necesaria para salvaguardar el derecho fundamental de libertad de prensa, que constituye un pilar importante de un Estado democrático. En este sentido, debe protegerse la identidad de la fuente de información periodística, por ejemplo, contra un titular de datos que solicitara acceder a sus datos personales, ya que podrían contener información sobre la fuente de los mismos (según el artículo 14 del Reglamento). Por otra parte, la rectificación de datos incorrectos publicados por los medios de comunicación debe seguir las normas del derecho a obtener rectificación asociado a la libertad de prensa.

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales dicha excepción debe aplicarse de manera restrictiva y no es aplicable a las bases de datos personales sin finalidad periodística aunque su responsable ejerza una actividad periodística (por ejemplo, a la base de datos de recursos humanos de un periódico).

– Tratamiento de datos con finalidad estadística

El artículo 28 de la Ley dispone lo siguiente:

«1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida en que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna».

El Grupo de Trabajo señala que no se trata tanto de una excepción al ámbito general de la legislación como de la aplicación del principio de protección de los datos personales, definidos en el artículo 2 de la Ley como «información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables». Por tanto, el Grupo de Trabajo interpreta que, cuando los titulares de datos son personas físicas o jurídicas determinadas o determinables, la legislación es aplicable plenamente y que ello justifica lo dispuesto en el artículo 28 del Reglamento que afirma que «los archivos, registros, bases o bancos de datos mencionados en el Art. 28

de la Ley n° 25.326 son responsables y pasibles de las multas previstas en el Art. 31 de la ley citada cuando infrinjan sus disposiciones».

### ***Ámbito territorial***

Este aspecto se regula en el artículo 44 de la Ley, según el cual puede establecerse la distinción siguiente:

#### *I. Normas de la Ley aplicables uniformemente en todo el territorio nacional:*

- Capítulo I: Disposiciones generales
- Capítulo II: Principios generales relativos a la protección de datos
- Capítulo III: Derechos de los titulares de datos
- Capítulo IV: (Obligaciones de los) usuarios y responsables de archivos, registros y bancos de datos
- Artículo 32: Sanciones penales
- La existencia y características principales del recurso judicial *habeas data* (tal como se establece en la Constitución)

#### *II. Normas de la Ley no aplicables uniformemente en todo el territorio nacional:*

- Capítulo V: Órgano de control
- Capítulo VI: Sanciones (que puede imponer el órgano de control)
- Capítulo VII: Acción de protección de los datos personales (*habeas data*): Procedimiento aplicable

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales en este ámbito son aplicables las normas siguientes:

- En cuanto a los archivos, registros y bases de datos interconectados en red a nivel interjurisdiccional (es decir, interprovincial), nacional o internacional: Se considera que estos casos competen a la jurisdicción federal y, por tanto, están sujetos a lo dispuesto en la Ley.
- En cuanto a otros tipos archivos, registros y bases de datos: Debe considerarse que dichos casos competen a la jurisdicción provincial y las provincias pueden legislar al respecto. Hasta la fecha, algunas provincias han legislado sobre el procedimiento del recurso *habeas data*.

### **1.2. Normas sectoriales**

Se incluyen normas sobre protección de datos en diferentes instrumentos jurídicos que regulan diversos sectores, como por ejemplo las transacciones con tarjeta de crédito, las estadísticas, la banca o la salud.

## **2. EVALUACIÓN DEL CARÁCTER APROPIADO DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA LEGISLACIÓN ARGENTINA**

El Grupo de Trabajo puntualiza que la presente evaluación del carácter apropiado de la legislación argentina sobre protección de datos se centra en las **normas generales** relativas a dicho ámbito mencionadas en el apartado precedente.

Se han comparado dichas normas con las disposiciones principales de la Directiva, teniendo en cuenta el dictamen del Grupo de Trabajo 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»<sup>5</sup>, que enumera diversos principios que constituyen «un “núcleo” de principios de “contenido” de protección de datos y de requisitos “de procedimiento/de aplicación”, cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección». El resultado del análisis es el siguiente:

## 2.1. Principios de contenido

### *Principios básicos*

- **Principio de limitación de objetivos** - los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por alguna de las razones contempladas en el artículo 13 de la Directiva.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el apartado 3 del artículo 4 de la Ley establece que «los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención».

- **Principio de proporcionalidad y de calidad de los datos** - los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, los apartados 4 y 5 del artículo 4 de la Ley establece que «los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. 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 art. 16 de la presente ley». Asimismo, el apartado 1 del artículo 4 de la Ley dispone que «los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos con relación al ámbito y finalidad para los que se hubieren obtenido».

- **Principio de transparencia** - debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder al apartado 2 del artículo 11 y al artículo 13 de la Directiva.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el artículo 6 de la Ley establece lo siguiente:

---

<sup>5</sup> WP 12 – Aprobado por el Grupo de Trabajo el 24 de julio de 1998, que puede consultarse en: [http://europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/index.htm](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm).

«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».

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales debe distinguirse entre la fuente de legitimidad del tratamiento y la obligación de informar al titular de los datos.

Por una parte, el tratamiento puede estar basado en diversos motivos lícitos, que están especificados en el artículo 5. Estos motivos incluyen, entre otros, el consentimiento del titular de los datos, la existencia de una fuente de acceso público, el ejercicio de tareas de interés público, una obligación legal o una relación contractual. Del artículo 5 del Reglamento se desprende que si el tratamiento se realiza con el consentimiento del titular, dicho consentimiento debe ser informado, lo que implica que previamente debe haberse facilitado al titular toda la información mencionada en el artículo 6.

Por otra parte, el artículo 6 de la Ley establece que «cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara (sigue una relación de cuestiones relativas al tratamiento)». Aunque la redacción de dicho artículo podría hacer pensar que la obligación de informar al titular de los datos se refiere a los casos en los que el titular facilita los datos por sí mismo y con su consentimiento, las autoridades argentinas señalan que dicha obligación es absoluta, incondicional y no depende del motivo que legitima el tratamiento. La obligación de informar es aplicable siempre, independientemente de si los datos personales se solicitan al titular o a un tercero y de si el tratamiento se realiza en virtud del consentimiento del titular o de cualquier otro motivo lícito incluido en el artículo 5 de la Ley. Por tanto, aunque el tratamiento se realice sin el consentimiento del titular, sigue siendo aplicable la obligación de informarle con arreglo al artículo 6 de la Ley.

- **Principio de seguridad** - el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el artículo 9 de la Ley establece lo siguiente:

« 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».

- **Derechos de acceso, rectificación y oposición** - el interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

En lo relativo al derecho de acceso, el Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el apartado 1 del artículo 14 de la Ley establece que «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». Este principio se desarrolla en los restantes apartados del artículo 14 y en el artículo 15 de la Ley, así como en los artículos 14 y 15 del Reglamento.

En cuanto al derecho de rectificación y oposición, el Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el apartado 1 del artículo 16 de la Ley establece que «toda persona tiene derecho a que sean rectificadas, 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». Este principio se desarrolla en los restantes apartados del artículo 16 de la Ley y en el artículo 16 del Reglamento.

Las excepciones a estos derechos, descritas en el artículo 17 de la Ley, permiten restricciones sólo para los bancos de datos públicos y por un número limitado de motivos importantes como la defensa nacional, el orden y la seguridad públicos, la protección de los derechos e intereses de terceros y cuando dicha información pudiera obstaculizar actuaciones judiciales o administrativas en curso vinculadas con 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. El Grupo de Trabajo considera que dichas excepciones se ajustan a lo dispuesto en el artículo 13 de la Directiva.

- **Restricciones respecto a transferencias sucesivas a otros terceros países** - únicamente deben permitirse transferencias sucesivas de datos personales del país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el apartado 1 del artículo 26 de la Directiva.

El Grupo de Trabajo entiende que la legislación argentina se ajusta en gran medida a este principio. En particular, el apartado 1 del artículo 12 establece que «es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuado».

El apartado 2 del artículo 12 de la Ley incluye excepciones a dicho principio en los casos siguientes:

- «a) Colaboración judicial internacional.
- b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inc. e) del artículo anterior.
- c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable.
- d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte.
- e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico».

El artículo 12 del Reglamento añade a la lista de excepciones el consentimiento expreso a la transferencia por parte del titular de los datos y la transferencia desde un registro público en las mismas condiciones que la consulta, en la línea establecida por la letra f) del apartado 1 del artículo 26 de la Directiva.

El Grupo de Trabajo considera que estas excepciones son más amplias que las previstas en la Directiva, especialmente que las enunciadas en las letras b), c) y d) del apartado 1 del artículo 12. El Grupo de Trabajo lamenta este hecho, preferiría que se limitaran dichas excepciones e invita al Gobierno argentino a trabajar en este sentido.

***Principios adicionales*** aplicables a tipos específicos de tratamiento son:

- **Datos sensibles** - cuando se trate de categorías de datos «sensibles» (las incluidas en el artículo 8 de la Directiva), deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el artículo 2 de la Ley define «datos sensibles» como «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». El artículo 7 de la Ley prevé protecciones adicionales para su tratamiento:

- «1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. 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.
3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. 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 respectivas».

Asimismo, el artículo 8 de la Ley establece que «los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los

pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional».

- **Márketing directo** - en el caso de que el objetivo de la transferencia de datos sea el márketing directo, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio. En particular, el artículo 27 de la Ley establece lo siguiente:

«1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa, y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo».

- **Decisión individual automatizada** - cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

El Grupo de Trabajo entiende que la legislación argentina se ajusta a este principio en lo relativo a las operaciones de tratamiento realizadas por el sector público, dado que tales decisiones automatizadas están prohibidas. En particular, el artículo 20 de la Ley establece lo siguiente:

«1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos».

En cuanto al sector privado, el Grupo de Trabajo observa que la legislación argentina no hace referencia a este aspecto. Sin embargo, el Grupo de Trabajo recuerda que una resolución de conformidad debe tener en cuenta todas las circunstancias que rodean a la transferencia de datos personales, y el nivel de riesgo que la transferencia plantea al titular de los datos es un elemento importante dentro de dichas «circunstancias». La legislación argentina prevé garantías para el titular en la prestación de servicios de información crediticia, que es un sector destacado en lo relativo a las decisiones individuales automatizadas. Dichas garantías, descritas en el artículo 26 de la Ley y del Reglamento, limitan las categorías de datos que pueden procesarse, la fuente de los datos y el período de tiempo al que pueden hacer referencia. Por tanto, el Grupo de Trabajo considera que la ausencia de una disposición general sobre decisiones individuales automatizadas para el sector privado no debe representar un obstáculo para una resolución de conformidad.

## 2.2. Mecanismos del procedimiento/de aplicación

El dictamen de 1998 del Grupo de Trabajo señala que para evaluar el carácter adecuado del sistema jurídico de terceros países, es necesario distinguir los objetivos subyacentes de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimiento judiciales y no judiciales utilizados en terceros países.

Los objetivos de un sistema de protección de datos son básicamente tres:

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

- **Ofrecer un nivel satisfactorio de cumplimiento de las normas** - Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la administración encargados específicamente de la protección de datos.

El Grupo de Trabajo entiende que la legislación argentina ha establecido diversos elementos encaminados a cumplir dicho objetivo. En particular:

### *(a) Sanciones efectivas y disuasorias*

La legislación argentina establece sanciones de diversos tipos y grados, en función de la gravedad de la infracción cometida por los responsables o usuarios de las bases de datos. Pueden identificarse dos categorías de sanciones:

#### *i. Sanciones administrativas*

Estas sanciones están reguladas en el artículo 31 de la Ley y el Reglamento y pueden consistir en apercibimiento, suspensión, multa de mil pesos (\$ 1 000) a cien mil pesos (\$ 100 000), clausura o cancelación del archivo, registro o banco de datos. Dichas sanciones podrán ser impuestas por el organismo de control y deberán graduarse atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceros y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora.

Asimismo, los responsables o usuarios de bancos de datos públicos pueden incurrir en responsabilidades administrativas en virtud de las normas generales de servicio público.

#### *ii. Sanciones penales*

El Código Penal argentino considera que tratar a sabiendas datos falsos o violar la confidencialidad o seguridad de los datos son infracciones penales. El Código prevé penas de prisión de 3 a 6 años (o de 4 años y medio a 9 años cuando del hecho se derive perjuicio a alguna persona) y la inhabilitación para desempeñar cargos públicos en el caso de los funcionarios.

El Grupo de Trabajo entiende que dichas sanciones son efectivas y disuasorias, y que pueden inducir de forma satisfactoria a desistir de tratar ilegalmente datos personales.

***(b) El órgano de control de protección de datos***

La legislación argentina prevé la creación de un órgano de control de protección de datos. Con arreglo al artículo 29 de la Ley, el órgano de control deberá realizar todas las acciones necesarias para cumplir los objetivos y demás disposiciones de la Ley. A tal efecto, el órgano de control ejercerá diversas funciones, entre las que se incluyen funciones de asistencia y asesoramiento, la adopción de normas y reglamentaciones en el desarrollo de la Ley, el mantenimiento de un censo de bases de datos y el control de la observancia de la legislación por parte de las bases de datos. El órgano de control goza de diversas atribuciones, como solicitar autorización judicial para acceder a locales o equipos de tratamiento de datos, solicitar información a las entidades públicas y privadas, imponer sanciones administrativas, constituirse en querellante en acciones penales y controlar el cumplimiento de los requisitos y garantías para inscribir bancos de datos privados en el Registro.

En virtud del artículo 29 del Reglamento, se creó la Dirección Nacional de Protección de Datos Personales (DNPDP), en el ámbito del Ministerio de Justicia y Derechos Humanos, como órgano de control. El Director ejercerá sus funciones con plena independencia, sin estar sujeto a instrucciones. Sus decisiones pueden recurrirse ante los tribunales con arreglo a las normas generales de procedimientos administrativos.

Sin embargo, el Grupo de Trabajo resalta que el Director del órgano de control de protección de datos es designado y puede ser destituido por el Ministerio de Justicia y Derechos Humanos, que también decide sobre el personal de dicho organismo, integrado en la estructura del Ministerio de Justicia. El Grupo de Trabajo considera que tal situación no garantiza que el organismo pueda actuar con plena independencia y, por tanto, insta a implementar los elementos necesarios a tal efecto, incluido un cambio en el procedimiento para designar y destituir al Director del organismo.

Con arreglo al artículo 44 de la Ley, el Grupo de Trabajo entiende que la DNPDP puede considerarse «jurisdicción federal» y que, por tanto, será responsable de controlar los registros, archivos o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional. En otros casos, dichos registros, archivos o bancos de datos estarán bajo jurisdicción provincial y, por tanto, fuera de la jurisdicción de la DNPDP. El Grupo de Trabajo invita a crear órganos de control de protección de datos en todas las provincias, ya que es importante para garantizar que en todos los casos exista un sistema de verificación directo por parte de la administración y un mecanismo institucional que permita investigar las denuncias de manera independiente de la vía judicial.

A la vista de estas consideraciones, el Grupo de Trabajo entiende que la legislación argentina incluye los elementos necesarios para ofrecer un buen nivel de cumplimiento de las normas.

- **Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos** - El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

El grupo de Trabajo observa que la legislación argentina ha establecido diversos elementos encaminados a cumplir este objetivo. En particular:

**(a) *El recurso judicial habeas data***

Como se ha mencionado anteriormente, la Constitución argentina prevé un recurso judicial especial para proteger los datos personales, conocido como «*habeas data*». Se trata de un subtipo 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. En particular, el tercer párrafo del artículo 43 de la Constitución argentina establece que «toda persona podrá interponer esta acción (es decir, el *habeas data*) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística».

Las normas legislativas que promulgan dicho recurso constitucional están incluídas en los artículos 33 a 43 de la Ley. El *habeas data* está concebido como un recurso judicial simplificado y rápido que los titulares de datos pueden utilizar contra los responsables o usuarios de bases de datos. El Gobierno argentino ha aclarado que, de acuerdo con lo comentado en relación al ámbito de la protección de datos en la legislación argentina, este recurso puede utilizarse contra los responsables o usuarios de cualquier base de datos pública o privada (y no sólo de bases de datos privadas destinadas a dar informes), si exceden el uso exclusivamente personal. Dicho aspecto ha sido confirmado por sentencias judiciales en este sentido.

El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto, según las cuales la Ley amplía el ámbito de lo dispuesto en la Constitución, al permitir utilizar dicho recurso en los casos en que se presuma el tratamiento de datos personales cuyo registro está prohibido por la Ley. Esto significa que cualquier infracción de las normas de protección de datos puede permitir utilizar el *habeas data*.

Asimismo, el Grupo de Trabajo observa que, en caso de alegar una excepción al derecho de acceso, rectificación o supresión, la carga de la prueba recae sobre el responsable o usuario de los datos.

El recurso *habeas data* permite que una sentencia judicial obligue a suprimir, rectificar, actualizar o declarar confidenciales los datos. El Grupo de Trabajo destaca que la sentencia judicial debe comunicarse al órgano de control, y que ello puede permitir que la DNPDP, en el ámbito de sus competencias, haga aplicar las normas de

protección de datos con respecto a otros titulares de datos afectados que pueden no haber tomado parte en el procedimiento inicial de *habeas data*.

### ***(b) Recursos judiciales generales***

Además del *habeas data*, las normas generales de la legislación argentina permiten hacer valer ante los tribunales con arreglo a los procedimientos generales los derechos y obligaciones relativos a la protección de datos. En particular, el titular de los datos puede incoar un proceso judicial ante un tribunal civil para obtener una compensación por los daños sufridos o para hacer cumplir cualquiera de los derechos reconocidos por la Ley o el Reglamento. Asimismo, pueden incoarse acciones penales por delitos relacionados con el tratamiento de datos personales incluidos en el Código Penal.

A la vista de estas consideraciones, el Grupo de Trabajo entiende que la legislación argentina incluye los elementos necesarios para ofrecer apoyo y asistencia a los titulares de datos individuales en el ejercicio de sus derechos.

- **Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas** - Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

El Grupo de Trabajo señala que ni la Ley ni el Reglamento incluyen normas específicas sobre el derecho de quienes resulten perjudicados por una operación de tratamiento ilegal a ser compensados por los daños sufridos. El Grupo de Trabajo toma nota de las explicaciones de las autoridades argentinas al respecto según las cuales, en ausencia de normas especiales, son aplicables las normas generales de la legislación argentina en materia de responsabilidad. Según el caso, pueden ser aplicables las normas en materia de responsabilidad contractual (si el tratamiento se realiza en el marco de una relación contractual entre las partes) o en materia de responsabilidad extracontractual en los demás casos. Las normas argentinas se ajustan en ambos casos a la tradición europea en materia de Derecho Civil y al principio que exige la compensación de los daños ocasionados en caso de manipulación ilegal.

A la vista de estas consideraciones, el Grupo de Trabajo entiende que la legislación argentina incluye los elementos necesarios para ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

### **2.3. Otros aspectos**

El Grupo de Trabajo observa que el artículo 5 de la Ley permite el tratamiento de datos personales sin el consentimiento del titular de los datos si los datos se obtienen de fuentes de acceso público irrestricto. El Grupo de Trabajo considera que es necesario establecer normas que garanticen que los datos incluidos en una fuente de acceso público irrestricto sean de tal naturaleza que no sea probable que su tratamiento sin el consentimiento del titular pueda suponer un riesgo para los derechos fundamentales y las libertades del individuo y, concretamente, para su derecho a la intimidad. Se sobreentiende que, incluso en el caso de que se incluyan datos personales en una fuente de acceso público irrestricto, es aplicable todo lo dispuesto en la legislación argentina sobre protección de datos.

### 3. RESULTADO DE LA EVALUACIÓN

El Grupo de Trabajo insiste en que, para llevar a cabo la presente evaluación de la legislación argentina, el Gobierno de dicho país ha facilitado información sobre la manera en que debe interpretarse lo dispuesto en la Constitución, la Ley y el Reglamento, y ha garantizado que las normas en materia de protección de datos se aplican conforme a dicha interpretación. Por tanto, el Grupo de Trabajo ha basado su análisis en las citadas informaciones y garantías del Gobierno argentino, y su dictamen está subordinado al hecho de que, en la aplicación efectiva de las normas de protección de datos en Argentina, se confirmen los citados elementos facilitados por el Gobierno de dicho país. En particular, en lo relativo al ámbito de la legislación argentina, el Grupo de Trabajo ha tenido especialmente en cuenta las explicaciones y garantías proporcionadas por las autoridades argentinas sobre la forma en que debe interpretarse lo dispuesto en la Constitución, la Ley y el Reglamento y sobre las situaciones a las que se aplica la legislación de protección de datos. La redacción del presente dictamen se ha basado en dichos supuestos y explicaciones, y no en una experiencia sólida en la aplicación práctica de la legislación, ni a nivel federal ni provincial. Esto es cierto también en lo relativo a que las autoridades argentinas tomen efectivamente en consideración, en un plazo razonable, las reservas expresadas anteriormente y las invitaciones a mejorar o modificar los textos legales vigentes.

**Como conclusión**, en virtud de todo lo anterior, el Grupo de Trabajo asume que Argentina garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el apartado 6 del artículo 25 de 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.

Sin embargo, el Grupo de Trabajo invita también a las autoridades argentinas a tomar las medidas necesarias para solucionar los puntos débiles de los actuales instrumentos legales identificados en el presente dictamen y solicita a la Comisión Europea continuar el diálogo con el Gobierno argentino con el citado objetivo. En particular, el Grupo de Trabajo insta a las autoridades argentinas a garantizar la aplicación efectiva de la legislación a nivel provincial mediante la creación de los necesarios órganos de control independientes en los casos en los que éstos no existan y, mientras tanto, a buscar soluciones temporales apropiadas que sean conformes con el orden constitucional argentino.

Hecho en Bruselas, el 3 de octubre de 2002

*Por el Grupo de Trabajo*  
*El Presidente*  
*Stefano RODOTA*