



0475/10/ES
WP 177

**Dictamen 6/2010, sobre el nivel de protección de datos personales en la
República Oriental del Uruguay**

Adoptado el 12 de octubre de 2010

Este Grupo de Trabajo fue creado, con arreglo al artículo 29 de la Directiva 95/46/CE, como un órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

La secretaría corre a cargo de la Dirección C (Derechos Fundamentales y Ciudadanía de la Unión) de la Comisión Europea, Dirección General de Justicia, B-1049 Bruselas, Bélgica, despacho MO-59 06/036.

Sitio internet: http://ec.europa.eu/justice/policies/privacy/index_en.htm

El Grupo de Trabajo sobre 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 y, en particular, sus artículos 29 y 30, apartado 1, letra b),

Visto el Reglamento del Grupo de Trabajo y, en particular, sus artículos 12 y 14,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

1. INTRODUCCIÓN

El 20 de octubre de 2008, la Misión de la República Oriental del Uruguay (en lo sucesivo, «Uruguay») ante la Unión Europea envió una carta a la Comisión Europea para transmitir la solicitud oficial del Gobierno uruguayo de que iniciara el procedimiento de declaración de que Uruguay ofrece un nivel adecuado de protección en lo que respecta a la transferencia de datos personales procedentes de la UE y el EEE, a tenor del artículo 25, apartado 6, de la Directiva 95/46/CE, relativa a la protección de datos personales (la «Directiva»).

A fin de evaluar si Uruguay ofrece un nivel adecuado de protección, la Comisión solicitó un informe al *Centre de Recherches Informatique et Droit* (CRID) de la Universidad de Namur. En este largo informe se analiza el grado de cumplimiento en el sistema normativo uruguayo de los requisitos de legislación sustantiva y de desarrollo de mecanismos de protección de datos personales fijados en el documento de trabajo «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de protección de datos de la UE», adoptado por el Grupo de Trabajo creado en relación con el artículo 29 de la Directiva el 24 de julio de 1998 (documento WP12). Las autoridades uruguayas, a través de la Unidad Reguladora y de Control de Datos Personales (URCDP), formularon sus observaciones en respuesta a las cuestiones planteadas en ese informe, mediante acuerdo de su Comité Ejecutivo del 11 de febrero de 2010.

Dicho informe, junto con las observaciones de las autoridades uruguayas, fueron evaluados por un Subgrupo creado específicamente para este fin en el seno del Grupo de Trabajo del artículo 29, el cual sometió a la consideración del Grupo el envío de una carta de su Presidente a las citadas autoridades uruguayas en la que, tras manifestar su valoración positiva del régimen de protección de datos de Uruguay (principalmente constituido por la Ley n.º 18.331, de 11 de agosto, de Protección de Datos personales y Acción de «Habeas Data» (la LPDP) y el Decreto de 31 de agosto de 2009, por el que se desarrolla dicha Ley (el DPDP), se comunicaban a las autoridades las cuestiones necesitadas de aclaración.

Las autoridades uruguayas enviaron al Grupo de Trabajo del artículo 29, a través de la URCDP, un extenso informe aprobado mediante acuerdo de su Consejo Ejecutivo de 23 de junio de 2010, en el que se daban respuesta a las cuestiones planteadas en la carta.

Se adjuntaba al informe una serie de documentos sobre la situación del país en materia de protección de datos personales, incluida su memoria anual de 2009 y su informe de actividades a 31 de mayo de 2010, diversos acuerdos del Consejo Ejecutivo y resoluciones relevantes sobre la cuestión de la protección de los datos personales.

El informe se distribuyó en septiembre de 2010 a los miembros del Subgrupo, quienes lo analizaron, prestando especial atención a las cuestiones planteadas en la carta enviada por el Grupo de Trabajo a las autoridades uruguayas. Una vez analizada la información, el Subgrupo consideró posible presentar sin más demora el presente documento al Grupo de Trabajo.

2. LA LEGISLACIÓN DE PROTECCIÓN DE DATOS DE URUGUAY

La Constitución Política de la República Oriental del Uruguay, aprobada en 1967, no reconoce expresamente los derechos a la intimidad y a la protección de los datos personales. En todo caso, la norma suprema tampoco se expresa de manera exacta en esta materia, ya que el artículo 72 establece que «[l]a enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno».

Por otra parte, el 332 establece que «[l]os preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales del Derecho y a las doctrinas generalmente admitidas.»

El Grupo de Trabajo confirma, por tanto, que estas dos cláusulas abiertas reconocen la existencia de derechos fundamentales de la persona no recogidos expresamente en la Constitución. Esta conclusión se ve ratificada por el artículo 1 de la Ley 18.331, de Protección de Datos personales y Acción de Habeas Data (LPDP), en el que se establece con absoluta claridad que «el derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el [artículo 72 de la Constitución de la República](#).»

Conforme a lo anterior, el derecho fundamental a la protección de los datos personales, reconocido como tal por el ordenamiento jurídico uruguayo, está regulado en la LPDP, promulgada el 11 de agosto de 2008, que sustituye a la anterior Ley de Protección de Datos Personales empleados en los Informes Comerciales y Acción de «Habeas Data» de 2004 y que regula actualmente, por tanto, en su totalidad esta materia en todos los sectores de actividad. Así, en su artículo 3 establece, como principio general, que «[e]l régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.»

Posteriormente, con el fin de desarrollar las disposiciones de la citada LPDP, el Gobierno de la República aprobó el Decreto de desarrollo de 31 de agosto de 2009 (el «DPDP»), cuyo preámbulo declara que «es conveniente la adecuación del ordenamiento jurídico nacional en la materia al régimen de derecho comparado de mayor recibo, fundamentalmente el consagrado por los países europeos a través 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 éstos.»

El Decreto introduce algunas aclaraciones y desarrollos reglamentarios de determinadas disposiciones de la LPDP. En particular, el Grupo de Trabajo considera necesario hacer referencia a los relativos al ámbito territorial de aplicación de la LPDP, la seguridad, el ejercicio de los derechos de acceso, actualización, inclusión y supresión de datos, y la regulación detallada de la organización, facultades y funcionamiento del Órgano de Control, denominado Unidad Reguladora y de Control de Datos Personales (URCDP).

Por último, el Grupo de Trabajo desea resaltar que la documentación remitida por las autoridades uruguayas en respuesta a la carta incluye la resolución del Consejo Ejecutivo de la URCDP en la que se acuerda *«trabajar para conseguir que el Ministerio de Relaciones Exteriores inicie los trámites necesarios ante el Consejo de Europa para los fines señalados en esta resolución, conforme al artículo 23 del Convenio 108 del Consejo de Europa (Convenio de Estrasburgo) y su Protocolo adicional de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.»*

3. EVALUACIÓN DE LA ADECUACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES OTORGADA POR LA LEGISLACIÓN DE PROTECCIÓN DE DATOS DE URUGUAY

La evaluación de la adecuación de la legislación de protección de datos personales vigente en Uruguay realizada por el Grupo de Trabajo se refiere fundamentalmente a la Ley n.º 18.331, de 13 de agosto, de Protección de Datos personales y Acción de Habeas Data (LPDP), y a su Decreto de desarrollo de 31 de agosto (DPDP).

Se han comparado los preceptos de esta Ley con las disposiciones principales de la Directiva, teniendo en cuenta el informe del Grupo de Trabajo WP12. Este informe establece una serie de principios que constituyen el *«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.*

3.1 Ámbito de aplicación de la normativa

Desde un punto de vista objetivo, como se ha indicado, el artículo 3 de la LPDP, reproducido en el artículo 2 del DPDP, establece como principio que este régimen regulador *«será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.»* La normativa de protección de datos será también aplicable por extensión, conforme al artículo 2, a las personas jurídicas, en cuanto corresponda.

El Grupo de Trabajo agradece las aclaraciones de las autoridades uruguayas en respuesta a sus dudas sobre la no aplicabilidad de la Ley a las *«bases de datos creadas y reguladas por leyes especiales.»*

Sobre esta cuestión, las autoridades uruguayas han señalado que las leyes especiales citadas, de las cuales ofrecen una serie de ejemplos, establecen un sistema de protección de datos más exigente que el de la Ley general, la cual, en cualquier caso, se aplicará también a las cuestiones no reguladas por la legislación específica, conforme al citado artículo 322 de la Constitución.

En cuanto al ámbito de aplicación territorial de la ley, el Grupo de Trabajo ha comprobado que el DPDP contiene expresamente un artículo al respecto que establece un régimen sustancialmente igual al previsto en el artículo 4 de la Directiva, lo que supone una garantía de cumplimiento de los principios y, en particular, del de limitación de las transferencias posteriores.

Así, el citado artículo 3 considera que el tratamiento de datos personales está sujeto a la LPDP cuando:

- sea efectuado por un responsable de base de datos o tratamiento establecido en el Uruguay, siendo éste el lugar donde ejerza su actividad, cualquiera que sea su forma jurídica.
- el responsable de la base de datos o tratamiento no esté establecido en territorio uruguayo pero utilice en el tratamiento de datos medios situados en el país.

A continuación, se establece una excepción a esta segunda regla para «los casos en que los citados medios se utilicen exclusivamente con fines de tránsito, siempre que el responsable de la base de datos o tratamiento designe un representante, con domicilio y residencia permanente en territorio nacional, ante el Órgano de Control, a los efectos de cumplir con las obligaciones previstas por la Ley que se reglamenta y en esta reglamentación.»

Por tanto, en relación con las aclaraciones anteriormente mencionadas, el Grupo de Trabajo considera que el ámbito de aplicación de la legislación uruguaya de protección de datos es similar al establecido en la Directiva.

3.2. Principios de contenido

a) Principios esenciales

1) Principio de limitación de objetivos: los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse 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 una de las razones expuestas en el artículo 13 de la Directiva.

El Grupo de Trabajo ha comprobado que este principio está expresamente recogido en el artículo 5, letra c), de la LPDP, que establece expresamente que la actuación de los responsables de las bases de datos, tanto públicos como privados y, en general, de todos quienes actúen en relación a datos personales de terceros, deberá ajustarse al principio general de finalidad.

El artículo 6 de la Ley establece que «[l]as bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública» y el artículo 8 añade que «[l]os datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención».

La única excepción a este precepto es que «[l]a reglamentación determinará los casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya perimido tal necesidad o permanencia.» El artículo 37 del DPDP regula el procedimiento de autorización de la conservación de datos para fines históricos, estadísticos o científicos. El Grupo de Trabajo entiende que esta excepción es similar a la prevista en el artículo 6, apartado 1, letra b), de la Directiva.

Del mismo modo, el artículo 11 de la LPDP establece que «[a]quellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros.»

Por tanto, el Grupo de Trabajo considera que la legislación uruguaya cumple este principio.

2) 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 transfieran o para el que se tratan posteriormente.

A juicio del Grupo de Trabajo, este principio está regulado en el artículo 7 de la LPDP a través del denominado «principio de veracidad», situado entre los principios rectores básicos de la Ley en su artículo 5 b).

El mencionado artículo 7 establece que «[l]os datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, equívocos y no excesivos en relación con la finalidad para la cual se hubiesen obtenido. La recolección de los datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones de la presente ley.»

Por otra parte, la LPDP establece que «[l]os datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario», y añade que «[c]uando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley.»

Por último, el artículo 8 de la LPDP establece que «[l]os datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.»

El Grupo de Trabajo tiene también en cuenta las explicaciones de las autoridades uruguayas sobre la presunción de licitud del tratamiento del artículo 9, letra c), de la LPDP, en el que se establece que «[n]o será necesario el previo consentimiento cuando (...) se trate de listados cuyos datos se limiten en el caso de las personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.»

Las autoridades uruguayas aclaran, a este respecto, que la legitimidad derivada de este precepto no puede entenderse en ningún caso como algo diferente de los principios de legitimación, proporcionalidad y limitación del objetivo. Por tanto, aunque no sea necesario obtener el permiso de la persona afectada, el responsable sólo puede tratar los datos a que se hace referencia en este artículo cuando el tratamiento esté incluido en el ámbito de los objetivos explícitos y legítimos identificados y siempre que los datos sean adecuados, pertinentes y no excesivos con relación al objetivo señalado, sin que exista ninguna otra legitimación distinta al necesario cumplimiento de ambos principios.

Por todo lo expuesto, el Grupo de Trabajo considera que el principio de proporcionalidad y calidad de los datos está también recogido en la legislación uruguaya.

3) 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 a los artículos 11, apartado 23, y 13 de la Directiva.

El Grupo de Trabajo considera que la obligación de informar al interesado sobre el tratamiento de sus datos está recogida en el artículo 13 de la LPDP, conforme al cual cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca de:

- La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios.
- La existencia de la base de datos, electrónica o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.
- El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles.
- Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud.
- La posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

El Grupo de Trabajo confirma también que, si el tratamiento se basa en el consentimiento del interesado, este último deberá ser informado, conforme a lo exigido en los artículos 9 de la LPDP y 5 del DPDP. Este último especifica que «[c]uando se solicite el consentimiento del titular para la recolección y tratamiento de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos y el tipo de actividad desarrollada por el responsable de la base de datos o tratamiento. En caso contrario, el consentimiento será nulo.»

El Grupo de Trabajo tiene también en cuenta las aclaraciones facilitadas por las autoridades uruguayas sobre la obligación de informar en todos los casos al interesado. Por tanto, aunque los términos del artículo 13 puedan dar la impresión de que esa obligación sólo se refiere a los supuestos en que el interesado facilite los datos voluntariamente y con su consentimiento, las autoridades afirman que tal obligación es absoluta, incondicional e independiente del motivo que legitime el tratamiento. La obligación de informar al interesado se aplica en todos los casos, independientemente de que los datos personales se soliciten a este mismo o a un tercero y de que el tratamiento se realice en virtud de la autorización del titular o de otra persona.

Las autoridades uruguayas aclaran igualmente que, si los datos se obtienen a través de un tercero mediante una comunicación de datos, el interesado deberá ser previamente informado asimismo de esta transferencia por la persona o la entidad que los comunique, con indicación de los destinatarios de los datos transferidos, con arreglo al artículo 13 de la LPDP.

4) 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 resalta que entre los principios del artículo 5 de la LPDP se recoge, en su letra e), el de seguridad de los datos.

El artículo 10 de la Ley desarrolla tal principio estableciendo que «[e]l responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y la confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado,» y añade que «[q]ueda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.»

El artículo 7 del DPDP añade que «[t]anto el responsable como el encargado de la base de datos o tratamiento deberán proteger los datos personales que sometan a tratamiento, mediante aquellas medidas técnicas y organizativas que resulten idóneas para garantizar su integridad, confidencialidad y disponibilidad,» siendo la naturaleza del encargado del tratamiento idéntica a la definida en la Directiva.

El Grupo de Trabajo observa asimismo que el artículo 8 del DPDP establece la obligación de informar a los interesados de cualquier posible vulneración de la seguridad, estableciendo que «[c]uando el responsable o encargado de la base de datos o tratamiento conozca de la ocurrencia de vulneraciones de seguridad en cualquier fase del tratamiento que realice, que sean susceptibles de afectar de forma significativa los derechos de los interesados, deberán informarles de este extremo.»

Por último, el Grupo de Trabajo tiene en cuenta la regulación de la obligación de confidencialidad y secreto del artículo 11 de la LPDP para considerar que, de acuerdo con las indicaciones ofrecidas, la legislación uruguaya cumple el principio de seguridad con arreglo a lo establecido en el documento WP12.

5) 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 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 relación con el derecho de acceso, el artículo 14 de la LPDP establece que «[t]odo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico.»

Esta información «debe ser proporcionada dentro de los cinco días hábiles de haber sido solicitada. Vencido el plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas de acuerdo con esta ley, quedará habilitada la acción de hábeas data.» Por otra parte, «[l]a información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen»

El artículo 14 establece además que «[l]a 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» y «[l]a información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.»

El Grupo de Trabajo tiene en cuenta las aclaraciones de las autoridades uruguayas en el sentido de que, sin perjuicio de lo establecido en el artículo 9, letra d), del DPDP, la persona no está obligada a justificar su solicitud, bastando la comprobación de su identidad. En particular, el Grupo de Trabajo tiene en cuenta la resolución de la URCDP de 18 de junio de 2010 en la que se establece que «*para ejercitar el derecho de acceso establecido en el artículo 14 de la Ley n.º 18.331, de Protección de Datos Personales y Acción de Habeas Data, el responsable de la base de datos sólo podrá exigir como requisito para la petición la identificación del titular de los datos*».

En relación con otros derechos de las personas, el artículo 15 de la LPP establece que «[t]oda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular.»

La Ley añade que «[e]l responsable de la base de datos o del tratamiento deberá proceder a realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde,» para concluir que «[e]l incumplimiento de esta obligación por parte del responsable de la base de datos o del tratamiento o el vencimiento del plazo, habilitará al titular del dato a promover la acción de habeas data prevista en esta ley.»

El Grupo de Trabajo toma nota de las aclaraciones del DPDP, centradas inicialmente en las definiciones de los artículos 10 a 12.

El artículo 10 define el derecho de rectificación del modo siguiente: «[e]l derecho de rectificación es el que tiene el titular a que se modifiquen los datos que resulten ser inexactos o incompletos.» El derecho de actualización se define en el artículo 11 como «el que tiene el titular a que se modifiquen los datos que resulten inexactos a la fecha de ejercicio del derecho» y el derecho de inclusión se define en el artículo 12 como «el que tiene el titular a ser incorporado con la información correspondiente en una base de datos cuando se acredite un interés fundado.»

El artículo 13 se refiere al derecho de supresión como «el que tiene el titular a que se eliminen los datos cuya utilización por terceros resulte ilegítima, o que resulten ser inadecuados o excesivos.»

En relación con esta ley, el Grupo de Trabajo tiene en cuenta los puntos señalados por el CRID en los dos informes relativos a la adecuación de la protección de datos en Uruguay y, en particular, al apéndice relativo a la aplicación del DPDP, considerando que, mediante la regulación del derecho de supresión, la ley uruguaya reconoce el derecho de oposición en los términos del artículo 14 de la Directiva.

Con respecto a las excepciones al ejercicio de estos derechos, el Grupo de Trabajo considera coherentes con los principios de protección de datos aquellas que se basan en la necesidad de preservar la información por motivos históricos, estadísticos o científicos y con arreglo a la ley aplicable o como consecuencia de la continuación de las relaciones contractuales entre el responsable del tratamiento y el interesado que justifican el tratamiento de los datos.

El Grupo de Trabajo considera también que las excepciones del artículo 26 de la LPPD que tienen en cuenta «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» pueden considerarse similares a las establecidas en el artículo 13 de la Directiva. En particular, el Grupo de Trabajo tiene en cuenta que la propia Ley establece en su artículo 26 que «[e]l titular del dato al que se deniegue total o parcialmente el ejercicio de los derechos mencionados en los incisos anteriores podrá ponerlo en conocimiento del Órgano de Control, quien deberá asegurarse de la procedencia o improcedencia de la denegación.»

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

El Grupo de Trabajo observa que la ley uruguaya define el concepto de transferencia internacional de datos de modo similar al establecido por los Estados miembros, incluyendo no sólo la transferencia de datos a un responsable del tratamiento de los datos situado en otro país, sino también los casos de transmisión de los datos a un encargado del tratamiento.

Así resulta de las definiciones de exportación e importación de datos recogidas en las letras e) y f) del artículo 4 de DPDP. El exportador se define específicamente como la «persona física o jurídica, pública o privada, situada en territorio uruguayo que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos de carácter personal a otro país» y el importador es la «persona física o jurídica, pública o privada, receptora de los datos de otro país, en caso de transferencia internacional de éstos, ya sea responsable del tratamiento, encargada del tratamiento o tercero».

El artículo 23 de la LPDP establece como regla general que «[s]e prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia.» Los dos últimos apartados de este artículo añaden que «[s]in perjuicio de lo dispuesto en el primer inciso de este artículo, la Unidad Reguladora y de Control de Protección de Datos Personales podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a 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 de cláusulas contractuales apropiadas.»

Por tanto, el Grupo de Trabajo considera que estas reglas establecen un sistema regulador de las transferencias internacionales de datos similar al establecido en los artículos 25, apartado 1, y 26, apartado 2, de la Directiva.

El artículo 23 de la LPDP establece también dos listas de excepciones a la autorización. El Grupo de Trabajo considera que la segunda de estas listas coincide con las excepciones del artículo 26, apartado 2, de la Directiva, pues establece los siguientes supuestos excluidos de la autorización:

- Que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista.
- Que 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.

- Que 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.
- Que 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 el procedimiento judicial.
- Que la transferencia sea necesaria para la salvaguardia del interés vital del interesado.
- Que la transferencia tenga lugar desde un registro 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 su consulta.

El Grupo de Trabajo observa también que la primera lista incluye una serie de supuestos que no coinciden literalmente con los del artículo 26, apartado 1, de la Directiva. Esta lista prevé las siguientes exenciones de la autorización:

- a) Cooperación judicial internacional, de acuerdo al respectivo instrumento internacional, ya sea Tratado o Convención, atendidas las circunstancias del caso.
- b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado por razones de salud o higiene públicas.
- c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la legislación que les resulte aplicable.
- d) Acuerdos en el marco de tratados internacionales de los cuales la República Oriental del Uruguay sea parte.
- e) Cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

El Grupo de Trabajo recuerda su informe 4/2002, sobre el nivel de protección de los datos personales en Argentina, en el que se señala que las excepciones previstas en las letras b), c) y d) podrían, en una primera lectura, indicar la existencia de más excepciones que las fijadas en el artículo 26, apartado 1, de la Directiva, lo que afectaría a la aplicación de este principio.

No obstante, el Grupo de Trabajo acoge favorablemente las aclaraciones facilitadas por las autoridades uruguayas, según las cuales estas exenciones no pueden considerarse de aplicación más amplia que la establecida en el artículo 26, apartado 1.

Así, la excepción prevista en el apartado c) hace referencia a la existencia de una relación contractual entre el interesado y el exportador que exige necesariamente la transferencia internacional de los datos personales para su ejecución.

Las excepciones b) y d) se interpretarán siempre considerando la existencia de un interés público importante, la ratificación de un convenio internacional vinculante para Uruguay o cuestiones de salud pública en el marco del concepto general de «un interés público importante».

Atendiendo a ello, el Grupo de Trabajo acepta tales explicaciones, si bien recomienda la adopción de medidas para garantizar que las autoridades uruguayas aplican efectivamente esta interpretación de las normas analizadas.

b) Principios adicionales

El documento WP12 alude a ciertos principios que deben aplicarse a tipos específicos de tratamiento de datos, centrándose en los siguientes:

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

El Grupo de Trabajo considera que la legislación uruguaya de protección de datos cumple este principio.

El artículo 4, letra e), de la LPDP define los datos sensibles como «datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.» En particular, en relación con los datos relativos a la salud, la letra d) del mismo artículo precisa la definición en términos similares a los establecidos por el Tribunal de Justicia de la UE, señalando que los datos sensibles son «informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona,» y que «[e]ntre otros, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad o a su información genética.»

El artículo 18 de la LPDP establece como principio general que «[n]inguna persona puede ser obligada a proporcionar datos sensibles. Estos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular,» y añade que «[l]os datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares.»

El artículo 19 señala, en relación con los datos referentes a la salud, que «[l]os 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, la normativa específica y lo establecido en la presente ley,» y el artículo 17, en relación con la comunicación de los datos sanitarios, establece que el consentimiento de la persona sólo puede exceptuarse cuando «se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, 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.»

El artículo 18 prohíbe también «la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. Se exceptúan aquellos que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial o étnico, a la salud y a la vida sexual, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la comunicación de dichos datos precisará siempre el previo consentimiento del titular del dato.»

2) Mercadotecnia directa: en el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

El Grupo de Trabajo considera que este principio está recogido en el artículo 21 de la LPDP, relativo a los casos de «recopilación de domicilios, reparto de documentos, publicidad, venta u otras actividades análogas.»

Así, tras señalar que «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» y reconocer el libre ejercicio, en todos los casos, del derecho de acceso, el último párrafo del artículo establece claramente que «[e]l titular podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos a los que se refiere el presente artículo.»

3) 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 confirma que este principio general está expresamente recogido en el artículo 16 de la LPDP, basado en el principio general de que «[l]as personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos que les afecte de manera significativa, que se base en un tratamiento automatizado o no de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros.»

El apartado tercero de ese mismo artículo establece también un principio similar al recogido en el documento WP12, al señalar que «el afectado tendrá derecho a obtener información del responsable de la base de datos tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto.»

3.3. Mecanismos de procedimiento/de aplicación

El Dictamen WP12 del Grupo de Trabajo «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE» señala que, para evaluar el carácter adecuado de la protección ofrecida, es necesario distinguir los objetivos 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.

A este respecto, 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, y
- ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

a) 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 los 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 considera que la legislación uruguaya cumple este objetivo a través de diversas disposiciones, en particular las siguientes:

La Unidad Reguladora y de Control de Datos Personales (URCDP)

La LPDP crea, en su artículo 31, una autoridad de control en materia de protección de datos denominada «Unidad Reguladora y de Control de Datos Personales (URCDP), como «órgano descentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica.»

La AGESIC comprende a los organismos autónomos de la citada URCDP y la Unidad de Acceso a la Información Pública (UAIP).

El Grupo de Trabajo toma nota de las observaciones de las autoridades uruguayas sobre la existencia de las «unidades reguladoras», organismos autónomos incluidos en el organigrama del Estado, con autonomía técnica y no sujetos a ninguna clase de mandato o instrucciones en el ámbito de sus competencias, que es el generalmente reconocido en la legislación uruguaya para los organismos reguladores generales e industriales. La URCDP es similar, en cuanto a su organización, a las entidades creadas para fines de planificación de las telecomunicaciones, la energía y la información pública.

En cuanto a su estructura, la LPDP establece en el artículo 31 que la URCDP «[e]stará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus

antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.» El Grupo de Trabajo observa que la referencia al «Poder Ejecutivo» debe entenderse hecha a la Presidencia de la República y que este procedimiento de designación de los miembros del órgano de control es el establecido en la ley uruguaya.

El Consejo Ejecutivo estará asistido por un Consejo Consultivo integrado por cinco miembros:

- Una persona con reconocida trayectoria en la promoción y defensa de los derechos humanos, designado por el Poder Legislativo, que no podrá ser un Legislador en actividad.
- Un representante del Poder Judicial.
- Un representante del Ministerio Público.
- Un representante del área académica.
- Un representante del sector privado, que se elegirá en la forma establecida reglamentariamente.

Con respecto a la independencia de esta autoridad, el Grupo de Trabajo encuentra pruebas suficientes en la legislación uruguaya, especialmente desde la aprobación del DPDP, para considerar que es aplicable a la URCDP.

En primer lugar, la LPDP establece expresamente que los miembros del Consejo Ejecutivo «no recibirán órdenes ni instrucciones en el plano técnico»; las autoridades uruguayas han aclarado que esta expresión debe entenderse en su sentido más amplio posible.

Por otra parte, el artículo 29 del DPDP establece que «[l]a actuación administrativa de la URCDP se desarrollará con arreglo a los principios de imparcialidad, celeridad, eficacia, verdad material, informalismo, debido proceso, impulsión de oficio, buena fe, motivación de las decisiones y simplicidad, los que servirán de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la tramitación de cualquier asunto.»

Por su parte, en relación con el mandato de los miembros del Consejo Ejecutivo, la LPDP establece una duración temporal del cargo y limita expresamente la posibilidad de cese, disponiendo en su artículo 31 que «[a] excepción del Director Ejecutivo de la AGESIC, los miembros durarán cuatro años en sus cargos, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de sus sucesores, o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso.»

Al Grupo de Trabajo le complace constatar también que la regulación del DPDP refuerza el papel de los dos miembros del Consejo Ejecutivo distintos al Director Ejecutivo de la AGESIC, reduciendo el papel de este último y garantizando mayor independencia para el órgano de control.

En este sentido, el artículo 21 del DPDP establece que «[l]a Presidencia de la URCDP será rotativa anualmente entre los integrantes del Consejo Ejecutivo, a excepción del Director Ejecutivo de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). En ausencia temporal del Presidente de la URCDP, la Presidencia será ejercida en forma interina por el restante miembro nombrado por el Poder Ejecutivo,» con lo que se elimina cualquier posibilidad de que la presidencia del órgano recaiga en el Director Ejecutivo de la AGESIC.

Este hecho reviste especial importancia, dado que el artículo 24, letra a), del DPDP establece que las resoluciones se tomarán por mayoría, añadiendo que «[s]i se produjera empate, el asunto será tratado en la próxima sesión y si éste subsistiera, el voto del Presidente se computará doble.» Esto impide que las decisiones del órgano de control se basen únicamente en la postura discrepante del Director Ejecutivo de la AGESIC, cuyo mandato está sujeto a un régimen diferente al de los restantes miembros del Consejo Ejecutivo.

El Grupo de Trabajo constata también que las facultades del Presidente de la URCDP incluyen el deber de «[a]doptar las medidas que creyere conveniente en caso de urgencia, dando cuenta en la primera sesión del Consejo Ejecutivo y estando a lo que se resuelva.»

Por último, el Grupo de Trabajo acepta que la independencia del órgano de control se ha acreditado en la práctica, al no existir alteración en su actividad como consecuencia del cambio de gobierno producido en Uruguay en 2009, según puede observarse en la información suministrada por la URCDP sobre sus actividades en 2009 y 2010.

Con respecto a las facultades de la autoridad, el Grupo constata que son las mismas establecidas para las autoridades de control de protección de datos en el artículo 28 de la Directiva. El artículo 34 de la LPDP asigna a la URCDP «las siguientes funciones y atribuciones:

- Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente ley y de los medios legales de que disponen para la defensa de los derechos que esta garantiza.
- Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley.
- Realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos.
- Controlar la observancia de las normas sobre integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos, pudiendo a tales efectos realizar las actuaciones de inspección pertinentes.

- 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.
- Emitir opinión toda vez que le sea requerida por las autoridades competentes, incluyendo solicitudes relacionadas con el dictado de sanciones administrativas que correspondan por la violación a las disposiciones de esta ley, de los reglamentos o de las resoluciones que regulan el tratamiento de datos personales comprendidos en ésta.
- Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyectos de ley que refieran total o parcialmente a protección de datos personales.
- Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita.»

La LPDP incluye también, como se indica a continuación, normas específicas en materia de investigación, inspección y sanciones, y el DPDP establece reglas concretas para ciertos procedimientos ante la URCDP y, en particular, para el registro del tratamiento y la autorización de las transferencias internacionales de datos.

El Grupo de Trabajo desea señalar que la URCDP ha acreditado el ejercicio de estas facultades en diversa documentación suministrada durante el análisis de la adecuación de la protección de datos expuesta en este documento.

Por todos estos motivos, el Grupo de Trabajo considera que Uruguay dispone de una autoridad supervisora de protección de datos con la independencia necesaria y con capacidad de aplicación adecuada, en términos similares a los establecidos en el artículo 28 de la Directiva.

Medios de aplicación y sanción.

El artículo 12 de la LPDP establece que «[e]l responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley».

Una de las funciones asignadas a la URCDP en el artículo 34 letra e), es «[s]olicitar 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. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados.»

El artículo 35 de la LPDP, por su parte, establece la posibilidad de aplicar medidas coercitivas en caso de vulneración de la Ley, señalando que «[e]l órgano de control podrá imponer las siguientes medidas sancionadoras a los responsables de las bases de datos o encargados del tratamiento de datos personales en caso de que se violen las normas de la presente ley:

- a) Apercibimiento.
- b) Multa de hasta quinientas mil unidades indexadas.
- c) Suspensión de la base de datos respectiva. A tal efecto, se faculta a la AGESIC a promover ante los órganos jurisdiccionales competentes, la suspensión de las bases de datos, hasta por un lapso de seis días hábiles, respecto de los cuales se comprobare que infringen o transgredieren la presente ley.»

Las funciones coercitivas de la URCDP en esta materia están recogidas en el artículo 31 de la DPDP, que permite a este órgano de control:

- «Realizar las inspecciones que el Consejo Ejecutivo entienda pertinente, las que serán dispuestas por resolución fundada.
- Solicitar ante la justicia competente las medidas pertinentes, cuando exista riesgo de pérdida de la prueba. La solicitud de dichas medidas necesitará resolución fundada del Consejo Ejecutivo.
- Comunicar las actuaciones al responsable de la base de datos o tratamiento a efectos de otorgarle vista, confiriéndole un plazo de diez días, contados a partir del siguiente al de su notificación para evacuarla. Transcurrido el plazo establecido, se elevarán las actuaciones para resolución del Consejo Ejecutivo, el que tendrá un plazo de treinta días para expedirse. La resolución que recaiga será impugnabile de acuerdo con las normas vigentes en la materia.»

A la luz de lo expuesto, el Grupo de Trabajo considera que la legislación uruguaya incluye medidas de investigación y sancionadoras similares a las establecidas para las autoridades supervisoras de los Estados miembros en el artículo 28 de la Directiva.

b) 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 de Uruguay incluye varios mecanismos destinados a este fin.

En primer lugar, el artículo 34, letra a), de la LPDP establece que «[e]l órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley.» Una de sus funciones es «[a]sistir y asesorar a las personas que lo requieran acerca de los alcances de la presente ley y de los medios legales de que disponen para la defensa de los derechos que esta garantiza.»

Como consecuencia de esta actividad puede abrirse un procedimiento de investigación y, en su caso, procedimientos sancionadores, ya que el procedimiento puede ser iniciado por el propio órgano de control o a instancia del interesado, como establece el DPDP.

Por otra parte, el artículo 34, letra h), incluye también entre las funciones de la URDDP la de «[i]nformar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita», regulando los procedimientos de inscripción y los registros.

Junto a estas funciones, la legislación uruguaya prevé la adopción de medidas para aumentar el conocimiento de las normas de protección de datos entre los interesados y los obligados a cumplirlas.

Esto se logra, por ejemplo, mediante la transparencia en la divulgación de sus decisiones y dictámenes. A tal efecto, el artículo 25, apartado primero, del DPDP establece que «[l]a URCDP hará públicas las resoluciones que adopte, mediante la publicación en su sitio web, en forma posterior a la notificación. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan.»

Consideramos que el segundo canal de asistencia para los interesados en la protección de sus derechos lo constituye la acción de «habeas data» prevista en el capítulo VIII de la LPDP.

Así, el artículo 38 de la Ley establece que el interesado «podrá entablar la acción de protección de datos personales o habeas data contra todo responsable de una base de datos pública o privada, en los siguientes supuestos:

- Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley.
- Cuando haya solicitado al responsable de la base de datos o tratamiento su rectificación, actualización, eliminación, inclusión o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley.»

Esta es una acción judicial de tramitación rápida que puede ser ejercitada por el interesado o sus representantes legales y, en el caso de las personas fallecidas, sus sucesores universales. La acción se rige por la legislación procesal, con las particularidades establecidas en la LPDP.

Según el artículo 43 de la LPDP, «[l]a sentencia que haga lugar al habeas data deberá contener:

- La identificación concreta de la autoridad o el particular a quien se dirija y contra cuya acción, hecho u omisión se conceda el habeas data.

- La determinación precisa de lo que deba o no deba hacerse y el plazo por el cual dicha resolución regirá, si es que corresponde fijarlo.
- El plazo para el cumplimiento de lo dispuesto, que será fijado por el tribunal conforme las circunstancias de cada caso, y no será mayor de quince días corridos e ininterrumpidos, computados a partir de la notificación.»

A la luz de esta información, como ya se ha indicado, el Grupo de Trabajo considera que la legislación uruguaya ofrece mecanismos suficientes de asistencia y apoyo a los interesados.

c) 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 artículo 12 de la LPDP establece que «[e]l responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley».

El Grupo de Trabajo observa que, en virtud de lo dispuesto en este artículo y en las normas generales uruguayas de Derecho civil, en particular en su Código Civil, los interesados perjudicados por el tratamiento de sus datos personales pueden solicitar la reparación correspondiente. Esta reparación puede incluir la indemnización de los daños y perjuicios tanto materiales como morales.

Por tanto, el Grupo de Trabajo considera que la legislación uruguaya reconoce adecuadamente esta garantía.

4. RESULTADO DE LA EVALUACIÓN

En conclusión, y en línea con lo indicado, el Grupo de Trabajo considera que **la República Oriental del Uruguay garantiza un nivel adecuado de protección**, a tenor del artículo 25, apartado 6, 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.

El Grupo de Trabajo resalta asimismo que, en el marco de la decisión adoptada por la Comisión, realizará un estrecho seguimiento de la protección de datos en Uruguay y de la forma en que la Autoridad de Protección de Datos (la «URCDP») aplique los principios de protección de datos señalados en el documento WP12 y en el presente.

Hecho en Bruselas, 12 de octubre de 2010

Por el Grupo de Trabajo:
El Presidente
Jacob KOHNSTAMM