LOS PRINCIPIOS JURIDICOS EN LA PROTECCIÓN DE DATOS PERSONALES

Análisis comparativo de la Directiva de la Unión Europea, la Ley Española y la Ley Uruguaya

Dra. Esc. Prof. María José Viega[(*)]

1. Introducción

El presente trabajo tiene como objetivo la realización de un análisis comparativo de los principios de la protección de datos personales, tomando como base la normativa uruguaya, concretamente la Ley Nº 18.331 de 11 de agosto de 2008 y su decreto reglamentario Nº 414/2009 de 31 de agosto de 2009, relacionándola con la Ley española Nº 15/1999 de fecha 13 de diciembre de 1999 y el Real Decreto 1720/2007 de 21 de diciembre y la Directiva 95/46/CE de 24 de octubre de 1995.

Se ha elegido este tema debido a la importancia que entendemos tienen los principios generales del Derecho como soportes estructurales de los ordenamientos jurídicos, tanto nacionales como internacionales.

El profesor Alberto Ramón Real ha destacado que en todo sistema jurídico hay cantidad de reglas de gran generalidad, verdaderamente fundamentales, en el sentido de que a ellas pueden vincularse, de un modo directo o indirecto, una serie de soluciones expresas del Derecho positivo a la vez que pueden resolverse, mediante su aplicación, casos no previstos, que dichas normas regulan implícitamente[1].

El Dr. Carlos Delpiazzo agrega que se trata de verdaderos cimientos que cumplen la triple función de servir como criterio de interpretación de las normas escritas, de colmar las lagunas o vacíos normativos, y de

(*)**Directora de la Dirección de Derechos Ciudadanos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)**. Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Profesora de Informática Jurídica, Derecho Informático y Derecho Telemático (UDELAR). Ex - Profesora de Derecho de las Telecomunicaciones en Universidad de la Empresa. Cursos del Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico. Miembro de la International Technology Law Association. Miembro del Colegio de Abogados del Uruguay y de la Comisión de Derecho Tecnológico de la Asociación de Escribanos del Uruguay. Miembro del Instituto de Derecho Informático (UDELAR) y Coordinadora del Grupo de Jurisprudencia del mismo Instituto. Co-editora del Boletín Electrónico de Derecho y Tecnologías (www.viegasociados.com). Autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

[1] REAL Alberto Ramón. "Los principios generales de Derecho en la Constitución uruguaya". Montevideo, 1965. Página 16.

constituir el único medio de asegurar un mínimo de unidad dentro de la pluralidad de formas y de preceptos que por su propia dinámica tienden a la dispersión y al particularismo[2].

Distintas organizaciones, así como la doctrina, han listado los principios que entienden pertinentes en materia de protección de datos, a modo de ejemplo, la OCDE, la Red Iberoamericana de Protección de Datos, así como también se han establecido principios básicos en el documento de Estándares Internacionales de Protección de Datos aprobado en Madrid el 5 de noviembre de 2009.

La OCDE ha elaborado Directrices en las cuales destaca los siguientes principios.

1) Principio de limitación de recogida. Deberán existir límites para la recogida de datos personales y cualquiera de estos datos deberán obtenerse con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del sujeto implicado.

2) Principio de calidad de los datos. Los datos personales deberán ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales.

3) Principio de especificación del propósito. El propósito de la recogida de datos se deberá especificar a más tardar en el momento en que se produce dicha recogida, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificando en cada momento el cambio de objetivo.

4) Principio delimitación de uso. No se deberá divulgar, poner a disposición o usar los datos personales para propósitos que no cumplan lo expuesto en el apartado 9, excepto si se tiene el consentimiento del sujeto implicado o por imposición legal o de las autoridades.

5) Principio de salvaguardia de la seguridad. Se emplearán salvaguardias razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos.

6) Principio de transparencia. Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de datos personales, el

[2] DELPIAZZO Carlos y VIEGA María José. “Lecciones de Derecho Telemático. Tomo I”. Fundación de Cultura Universitaria, abril 2004. Página 73.

propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos.

7) Principio de participación individual. Todo individuo tendrá derecho a:

- que el controlador de datos u otra fuente le confirme que tiene datos sobre su persona;

- que se le comuniquen los datos relativos a su persona
  – en un tiempo razonable;
  – a un precio, si existiese, que no sea excesivo;
  – de forma razonable; y
  – de manera inteligible;

- que se le expliquen las razones por las que una petición suya según los sub apartados (a) y (b) haya sido denegada, así como poder cuestionar tal denegación; y

- expresar dudas sobre los datos relativos a su persona y, si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan.

8) Principio de responsabilidad. Sobre todo controlador de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

También la Red Iberoamericana de Protección de Datos elaboró unas Directrices para la armonización de la protección de datos en la comunidad iberoamericana, en la reunión realizada en Cartagena de Indias (Colombia) el 4 de Mayo de 2007, destacándose en este documento los siguientes principios:

Principios relacionados con la finalidad y calidad de los datos.

- Tratamiento leal y lícito: los datos sólo podrán ser recabados y tratados de buena fe, con estricto respeto por la Ley y los derechos de las personas y de conformidad a lo previsto en las presentes directrices.

- Limitación de la finalidad: los datos únicamente podrán ser recabados y tratados para el cumplimiento de las finalidades determinadas, explícitas y legítimas relacionadas con la actividad de quien los trate.

  No podrán ser tratados para fines distintos de aquéllos que motivaron su obtención a menos que exista legitimación suficiente para ello, conforme a lo establecido en el apartado 3 de estas directrices.

- Principio de proporcionalidad: Sólo podrán ser sometidos a tratamiento los datos que resulten adecuados, pertinentes y no excesivos en relación con las finalidades a las que se refiere el punto anterior.

- Principio de exactitud: Los datos deberán mantenerse exactos, completos y puestos al día, respondiendo a la verdadera situación de la persona a la que se refieran.

- Principio de conservación: Los datos deberán ser cancelados o convertidos en anónimos cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades que justificaron su obtención y tratamiento

También el Dr. Delpiazzo, al analizar los principios generales en materia de Derecho Telemático, analiza tres categorías: los estructuradores del mundo virtual, los relativos al comercio electrónico y los principios en materia de protección de datos personales[3].

1) Principio de justificación social, según el cual la recolección de datos deberá tener un propósito general y usos específicos socialmente aceptables.

2) Principio de limitación de la recolección, según el cual los datos deberán ser recolectados por medios lícitos y con conocimiento y consentimiento del interesado, acotándose al mínimo necesario para alcanzar el fin perseguido.

3) Principio de fidelidad de la información, los datos personales que se registren deberán ser exactos, completos y actuales, rectificándose o cancelándose en su caso.

4) Principio de especificación del propósito obliga a que en el momento de recolectarse los datos se informe con qué objetivo ello se hace, no pudiendo luego usarse para fines diferentes.

5) Principio de confidencialidad aboga porque el acceso a los datos por parte de terceros sólo podrá ser llevado a cabo con consentimiento del sujeto de los datos o con autorización legal.

6) Principio de salvaguarda de la seguridad obliga a que todo responsable del registro de datos personales deba adoptar las medidas de seguridad adecuadas para protegerlos contra posibles pérdidas, destrucciones o acceso no autorizado.

7) Principio de transparencia conduce a la diafanidad del obrar público y de todos quienes operen con datos personales, debiendo

[3] DELPIAZZO Carlos y VIEGA María José. “Lecciones de Derecho Telemático. Tomo I”. Ob. Cit. Página 75.

conocerse la existencia, fines, usos y métodos de operación de los registros de tales datos.

8) Principio de limitación determina que los datos personales no puedan conservarse más allá del tiempo requerido para alcanzar el objetivo para el cual fueron recolectados.

José Luis Piñar[4] entiende que los principios son: consentimiento, información, finalidad, calidad de los datos, con especial referencia a la proporcionalidad, seguridad. Principios todos ellos recogidos en la Ley Orgánica de Protección de Datos, artículos 4 y siguientes, a los que puede añadirse el de utilización leal de los datos y el de minimización en el uso de los datos (éste, por cierto, reconducible, también en mi opinión, al de proporcionalidad).

En esta línea de pensamiento, el artículo 5 de la ley uruguaya establece 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 a los siguientes principios generales:*

a) legalidad,

b) veracidad,

c) finalidad,

d) previo consentimiento informado,

e) seguridad de los datos,

f) reserva,

g) responsabilidad.

Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes".

Este artículo se entiende particularmente relevante, en la medida que destaca la importancia de éstos, estableciendo que son la brújula para interpretar y aplicar la ley.

OCDE	RIPD	Están	Dr.	Dr. José	Directiv	Ley	Ley

[4] MURILLO DE LA CUEVA Pablo Lucas. y PIÑAR MAÑAS José Luis. "El derecho a la autodeterminación informativa". Fundación Coloquio Jurídico Europeo. Madrid, 2009. Página 101

		dares Internacionales de PDP	Delpiazzo	Luis Piñar	a 95/46/CE	15/1999	18.331
Limitación de la recogida	Tratamiento leal y lícito	Lealtad y legalidad	Limitación de la recolección		Tratados de manera leal y lícita		Legalidad
Calidad de los datos: relevantes, exactos, completos y actuales	Exactitud	Proporcionalidad. Calidad	Fidelidad de la información	Calidad de los datos	Exactos y actualizados	Exactos, puestos al día y relevantes (art. 4 nº 3)	Veracidad
Especificación del propósito	Limitación de la finalidad	Finalidad	Especificación del propósito	Finalidad	Recogidos con fines determinados, explícitos y legítimos	No podrán usarse para finalidades incompatibles (art. 4 nº 2)	Finalidad
Delimitación de uso			Confidencialidad			Deber de secreto (art. 10)	Reserva
Salvaguarda de la seguridad			Salvaguarda de la seguridad	Seguridad			Seguridad de los datos
Transparencia		Transparencia	Transparencia				
Principio de participación individual							

Responsabilidad		Responsabilidad			Los responsables del tratamiento deberán garantizar el cumplimiento de lo dispuesto en el apartado 1.		Responsabilidad
	Proporcionalidad: adecuados, pertinentes y no excesivos			Proporcionalidad	Adecuados, pertinentes y no excesivos con relación a los fines	Adecuados, pertinentes y no excesivos (art. 4 nº 1)	Veracidad
	Conservación		Limitación del tiempo		Conservados durante un tiempo no mayor al necesario	Cancelados cuando dejen de ser necesarios (art. 4 nº 5)	Conservación (art. 8)
			Justificación social				
				Información			
				Consentimiento		Consentimiento inequívoco (art. 6.1)	Previo consentimiento informado

2. Principio de legalidad

La ley uruguaya regula en el artículo 6º el principio de legalidad estableciendo que: *"La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia.*

Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública".

A la legalidad hace referencia la RIPD y también la Directiva al establecer que los datos deben ser tratados de manera leal y lícita.

La LOPD define el tratamiento de datos en el artículo 3 c) y la Resolución de Madrid lo define como: "*cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión*".

Un ejemplo sobre este tema está dado por el expediente de la AEPD PS/00134/2008[5] que tuvo entrada por una denuncia contra la empresa LEX Company, quien se especializaba en la publicación de resoluciones judiciales a través de su página web. La empresa publicó una sentencia sin anonimizar los datos personales del denunciante, en la cual figuraban los apellidos, el DNI, su domicilio y la condición de denunciante en el juicio. La AEPD resolvió imponer a la empresa una multa de 6000 euros, por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3 d) de dicha norma, de conformidad con lo establecido en el artículo 45.2 y 5 de la citada Ley Orgánica.

La vertiente subjetiva del principio de tratamiento encuentra su fundamento en determinar quién está legitimado para llevar a cabo un determinado tratamiento de datos personales, así como los requisitos que debe cumplir. Conforme a la normativa europea, recogida en la LOPD, está legitimado para realizar un tratamiento de datos personales tanto el Responsable como el Encargado del mismo. El encargado de tratamiento es aquél que trata los datos por cuenta del responsable al que le presta servicios tratando los datos conforme a sus instrucciones[6].

[5] www.agpd.es/portalweb/resoluciones/procedimientos sancionadores/p 2009/index-ides-idphp.php

[6] LOPEZ CALVO, José, GARCIA PRIETO, Manuel, NAVARRO ALONSO Isabel y LOBATO LOBATO Angelina. *Módulo 2. Principios básicos de la protección de Datos*. Curso "El derechos a la protección de datos personales, 1º edición. Fundación CEDDET. Páginas 27 y 28.

Por otra parte, los Estándares sobre Protección de datos personales y privacidad, aprobados en Madrid el 5 de noviembre de 2009, enuncian bajo el título de Principio de lealtad y legalidad en los siguientes términos:

"Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas, de conformidad con lo previsto en el presente Documento y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos.

En particular, se considerarán desleales aquellos tratamientos de datos de carácter personal que den lugar a una discriminación injusta o arbitraria contra los interesados".

3. Principio de veracidad

El artículo 7° de la Ley N 18.331 regula lo referente al Principio de veracidad, estableciendo que los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido.

También hace referencia a que la recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley.

En los incisos finales dice que los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario y que cuando 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.

Como vemos, este artículo, regula varios aspectos considerados en la Directiva y en la Ley española en forma separada.

La normativa española refiere al principio de calidad de los datos, incluyendo proporcionalidad, veracidad y finalidad. Este principio se observa al momento de la recogida de datos, debido a que no podrán recabarse datos que no se adecuen a las exigencias derivadas del mismo, pero también en el tratamiento posterior.

El principio de calidad de los datos determina que:

a. El tratamiento de los datos debe ser legítimo y leal, como lo establece la Directiva 95/46/CE, por lo que deben ser recogidos por medios lícitos.

b. Proporcionalidad: solo pueden recabarse datos adecuados, pertinentes y no excesivos de acuerdo a la finalidad para la cual se obtengan. Sería excesivo solicitar datos de salud para abrir una cuenta bancaria. Como vemos este principio se encuentra ligado al principio de finalidad. El dato debe ser adecuado a la finalidad que lo motiva, debe ser pertinente para conseguir la finalidad que legitima su tratamiento y no pueden recabarse datos que no sean necesarios para la finalidad que se persigue, porque se considerarían excesivos.

A modo de ejemplo, una Sentencia de la Audiencia Nacional de fecha 16 de enero de 2008 declaró la confluencia de los citados elementos en la actuación de un centro médico que utilizó datos de salud. Para la solicitud de un préstamo hipotecario con una entidad bancaria, el interesado suscribió un seguro de vida. Al momento de la firma del seguro se le informó que se le realizarían las siguientes pruebas médicas: examen médico, análisis de orina, de sangre y electrocardiograma en reposo. Pero entre las pruebas que se le realizaron, se le hizo detección del SIDDA sin que hubiera sido informado en forma expresa. La sentencia considera que si bien la expresión fue "análisis de sangre" al momento de solicitar el consentimiento, si bien no se dijo expresamente, debía valorarse que es frecuente que se realice este tipo de análisis cuando se suscribe un seguro de vida, debido a los riesgos que resulta de la finalidad, por lo que concluye que este tratamiento fue adecuado, pertinente y no excesivo al existir entre la finalidad pretendida y la realización de la prueba del SIDA la necesaria coordinación.

El Tribunal Constitucional español, determinó en la Sentencia 207/1996 que: "para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: "*si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)*".

También la AEPD ha resuelto sobre este tema en el Informe 90/2009[7]. La cuestión planteada es si una empresa dedicada a prestar servicios de seguridad privada puede exigir a los escoltas que trabajan para ella que lleven de forma continuada un terminal de telefonía, para que la empresa pueda conocer la localización geográfica del empleado, aunque no se encuentre de servicio.

[7] www.agpd.es/portalweb/canaldocumentacion/informes juridicos/calidad/common/pdf/2009-0090_Proporcionaidad-en-el-tratamiento-de-datos-de-localizaci-oo-n.pdf

Los datos de localización, ya que permiten conocer la posición geográfica de una persona, constituyen datos personales y su tratamiento debe respetar los principios. En el caso del informe la finalidad era garantizar la seguridad de la persona escoltada. Por tanto el informe considera que se respeta el principio de proporcionalidad respecto a la utilización de esos datos en la jornada laboral, pero no respeta dicho principio el tratamiento de los datos de localización fuera del horario de trabajo, ya que la finalidad no requiere ese tratamiento.

El informe 368/2006[8] resuelve sobre si era lícito establecer un sistema de control para gestionar las ausencias y retrasos de los alumnos de un colegio, basado en la obtención de la huella dactilar de éstos. El informe concluye que la obtención de la huella dactilar para identificar a los alumnos de un centro resulta excesivo y desproporcionado para el fin que se persigue, ya que no se considera justificado el tratamiento de datos de menores para la finalidad pretendida.

c. Veracidad: los datos deben ser exactos y actuales. El responsable del fichero o tratamiento queda obligado a comprobar la exactitud de dato debiendo desarrollar esta obligación de forma diligente a fin de evitar, por un lado, que datos inexactos accedan a su fichero y, por otro, la existencia de inexactitudes en los datos ya registrados.

Un ejemplo respecto a este tema es la suplantación de identidad. Al respecto, puede citarse la experiencia de la Agencia Española de Protección de Datos. Estos supuestos se producen cuando, la empresa que vende el producto o presta el servicio, no contrata directamente con el cliente, sino que encomienda a una tercera empresa o persona la labor de captar clientes y obtener de ellos consentimiento para la contratación. Este tercero, en algunas ocasiones, con la finalidad de obtener su comisión, formaliza contratados, sin que el titular de los datos utilizados haya consentido la contratación, y presenta al responsable del fichero o tratamiento documentos que no han sido firmados por el verdadero titular de los datos. En definitiva este tercero recaba los datos en forma fraudulenta[9].

La Sentencia 3 de noviembre de 2004 de la Audiencia Nacional confirmó la sanción impuesta por la AEPD, a una empresa que incluyó en un fichero de solvencia patrimonial los datos de una persona, a pesar de que había sido exonerada por sentencia firme del pago de

---

[8] www.agpd.es/portalweb/canaldocumentacion/informes juridicos/calidad/common/pdfs/2006-0368_Proporcionalidad-del-tratamiento-de-la-huella-dactilar-de-alumnos-de-un-colegio.pdf

[9] LOPEZ CALVO, José, GARCIA PRIETO, Manuel, NAVARRO ALONSO Isabel y LOBATO LOBATO Angelina. *Módulo 2. Principios básicos de la protección de Datos*. Fundación CEDDET. Ob. Cit. Página 56.

una deuda que se le reclamaba. Establece la sentencia que el principio se infringe cuando se facilitan datos erróneos a un fichero que presta información a terceros sobre el incumplimiento de obligaciones dinerarias. En este caso, la información que se registró en el fichero de solvencia patrimonial no respondía verazmente a la situación del afectado dado que hacía referencia a su condición de deudor de una deuda de la había sido absuelto por sentencia firme.

Parece importante determinar si cualquier error supone una infracción al principio de calidad de los datos, ya que debemos estar ante un error relevante y no ante un mero error material que no tenga repercusiones externas, o sea que no ocasione un perjuicio al afectado.

Por ejemplo, el envío de una factura a una dirección anterior, o un dato identificatorio equivocado puede dar lugar al ejercicio del derecho de rectificación, y no será una vulneración al principio de calidad de los datos si el responsable actúa diligentemente cuando se detecte el error.

Si el que proporciona el dato erróneo es el propio interesado, el responsable del tratamiento no tiene responsabilidad, pero esto no exonera al responsable del fichero de realizar comprobaciones precisas, como por ejemplo la identidad de la persona que entrega los datos.

d. Finalidad: los datos solo podrán utilizarse para las finalidades para la cual fueron recogidos. Sobre el principio de finalidad ampliaremos en el punto siguiente.

Este principio de veracidad aparece en el Considerando 28 de la Directiva 95/46/CE que dice: "*Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal respecto al interesado; que debe referirse en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originariamente especificados*".

La ley uruguaya regula la calidad de los datos, en forma separada, pero la esencia es la misma.

4. Principio de finalidad

Establece el artículo 8 de nuestra ley, bajo el título Principio de finalidad que: *"Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.*

Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados.

La 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 aún cuando haya perimido tal necesidad o pertinencia.

Tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular".

El principio de finalidad conjuntamente con el previo consentimiento informado, constituyen a nuestro entender las bases fundamentales del sistema de protección de datos en Uruguay. Ambos son la garantía del derecho fundamental que se consagra en el artículo 1º de la ley, ya que permiten que las personas controlen sus datos y el uso que de ellos se realiza.

Una cuestión que se ha planteado es si pueden recabarse datos para cualquier finalidad. Se ha respondido en forma afirmativa, siempre que la finalidad a la que se destinen los datos sea determinada (no pueden ser finalidades genéricas), explícita (el tratamiento no puede tener finalidades confusas), legítima y que el afectado haya prestado su consentimiento para el tratamiento de sus datos con esa finalidad.

Establece el principio que los datos no pueden ser tratados para finalidades diferentes, pero es importante determinar cuando estamos ante un desvío de la finalidad. El Tribunal Constitucional español, en la sentencia de 13 de enero de 1998 analiza el caso de una empresa que ante la realización de una huelga, convocada por varios sindicatos, y debido al difícil seguimiento de la misma por parte de la empresa, utilizó el dato de afiliación sindical, facilitado por los trabajadores para el cobro de la cuota sindical, para practicar en las retribuciones correspondientes al mes en que se realizó la huelga la retención correspondiente al seguimiento de aquella. Dicho descuento se realizó en forma generalizada a las personas afiliadas a los sindicatos convocantes a la huelga, hubieran secundado o no. Se presumió la participación en la huelga por el hecho de pertenecer a un sindicato, atentando no sólo contra el derecho fundamental a la protección de datos, al utilizar datos especialmente protegidos para una finalidad distinta a aquella para la que fueron facilitados, sino también contra el derecho a la libertad sindical[10].

El artículo uruguayo refiere también a la eliminación de los datos cuando cesa la finalidad. Este tema fue tratado por el decreto reglamentario,

[10] LOPEZ CALVO, José, GARCIA PRIETO, Manuel, NAVARRO ALONSO Isabel y LOBATO LOBATO Angelina. *Módulo 2. Principios básicos de la protección de Datos*. Fundación CEDDET. Ob. Cit. Páginas 62 y 63.

definiendo y diferenciando en el artículo 4 bloqueo de datos y cancelación o supresión de datos:

A) Bloqueo de datos: procedimiento mediante el cual se reservan datos con el fin de impedir su tratamiento, excepto para ser puestos a disposición de los Poderes del Estado, o instituciones que estén legalmente habilitadas, a los efectos de atender las posibles responsabilidades surgidas del tratamiento.

B) Cancelación o Supresión de datos: procedimiento mediante el cual el responsable cesa en el uso de los datos. La supresión o cancelación implicará el bloqueo de dichos datos durante el plazo establecido en la normativa vigente; vencido éste se deberá proceder a su eliminación definitiva.

También el Real Decreto español en el artículo 5 b) define que se entiende por cancelación.

5. Principio del previo consentimiento informado

Como dijimos anteriormente, el artículo 9º es fundamental en nuestra normativa, al regular el Principio del previo consentimiento informado. Se establece que para que los datos personales puedan tratarse en forma lícita el titular debe haber prestado su consentimiento libre, previo, expreso e informado, el que, además, deberá documentarse.

En el inciso tercero, se señalan una serie de excepciones, pero se quiere hacer hincapié en que son excepciones solo al consentimiento, que como se ha dicho, es necesario que se encuentre documentado y por lo tanto es muy estricto su control. Por ese motivo, se exceptúa en los casos que se dirán, pero rigiendo en todo la ley para este tipo de datos. Tal es así, que aunque las bases de datos traten solo este tipo de datos personales, igualmente deben inscribirse ante el Órgano de Control.

No se requiere el previo consentimiento cuando:

a) *los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación;*

b) *se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;*

c) *se trate de listados cuyos datos se limiten en el caso de 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;*

d) deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento;

e) *se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico*".

En el decreto reglamentario Nº 414/2009 de 31 de agosto de 2009 se reguló expresamente el principio del previo consentimiento informado, estableciendo en el artículo 5 que el interesado debe ser informado inequívocamente de la finalidad en el tratamiento de datos y que en caso contrario el consentimiento será nulo.

El artículo 6 establece que debe facilitarse al titular un medio sencillo, claro y gratuito para que manifieste su consentimiento o la negativa al tratamiento de sus datos. En caso de formularios, deben existir dos opciones claras y que no se encuentren pre marcadas, a los efectos de que no existan confusiones para el titular de los datos.

En el inciso final establece que transcurridos diez días de recibida la solicitud de consentimiento, sin que el titular se manifieste, se entenderá que es una negativa al tratamiento. Esta norma es sumamente importante, porque no está admitiendo el consentimiento tácito y consagra, a diferencia de múltiples normas que establecen el silencio positivo, un silencio negativo.

Dice el Dr. Rebollo Delgado que el consentimiento para el tratamiento de datos es una facultad de libertad del individuo para decidir acerca de sus datos, aunque se encuentra muy mediatizada en la norma por el conjunto de excepciones a que se ve sometida. El art. 6.1 contiene una regla general y una excepción, también general, amparada en una disposición legal. Según la Agencia Española y las Recomendaciones emitidas por el Comité de Ministros del Consejo de Europa son los siguientes: libertad en la prestación el consentimiento, específico, informado e inequívoco y expreso para el caso de los datos sensible. Otra regla general es la revocación del consentimiento para los casos en que la entrega de los datos se realiza en forma libre, con la inexistencia de efectos retroactivos[11].

También la ley española plantea una serie de excepciones al consentimiento, que son las siguientes:

a) art. 6.2 de la LOPD – Además de la excepción general del art. 6.1 referida a la existencia de una ley, no será preciso el consentimiento cuando los datos se recojan en los siguientes supuestos: "*para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean*

[11] Rebollo Delgado, L y Serrano Pérez M: *Introducción a la protección de datos*. 2ª Ed. Madrid 2008, pág. 127.

necesarios para su mantenimiento o cumplimiento, cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del art. 7 apartado 6, de la presente ley, o cuando los datos figuren en fuentes públicas accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

b) Art. 22.2 de la LOPD – Permite la recogida y tratamiento de datos de carácter personal por las Fuerzas y Cuerpos de la Seguridad para fines policiales sin consentimiento de las personas afectadas, limitándose a aquellas categorías de datos necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales. Este artículo ha sido criticado por numerosos autores por la utilización abusiva de conceptos indeterminados.

En el derecho español la forma de otorgar el consentimiento depende del tipo de datos especialmente protegidos de que se trate:

a) Relativos a la ideología, afiliación sindical, religión y creencias, en este caso es necesario el consentimiento expreso y por escrito del afectado.

b) Relativos al origen racial, a la salud y a la vida sexual. En este caso para realizar el tratamiento es necesario que lo disponga una norma de rango legal o que el afectado lo consienta expresamente.

A modo de ejemplo sobre la complejidad de estos temas, se plantea el apartado 5 de la Memoria Explicativa del Convenio 108 de Europa que define "datos personales relativos a la salud". También se encuentra definido en la Recomendación R(97)5 del Comité de Ministros del Consejo de Europa, y el propio Tribunal de Justicia de las Comunidades Europeas, Sala Pleno, de 6 de noviembre de 2003, asunto C-101/2001 (Caso Lindqvist), así como la propia normativa española en su artículo 5.1g) del reglamento que desarrolla la LOPD. En todas las definiciones se afirma que este tipo de datos comprende la información relativa a todos los aspectos de la salud pasada, presente y futura, tanto físicos como síquicos, de una persona, incluida la información genética[12].

Prácticamente idéntica es la definición que consagra el artículo 4 literal d) del decreto reglamentario uruguayo: "*Dato personal relacionado con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona. Entre otros, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad o a su información genética*".

[12] LOPEZ CALVO, José, GARCIA PRIETO, Manuel, NAVARRO ALONSO Isabel y LOBATO LOBATO Angelina. *Módulo 2. Principios básicos de la protección de Datos*. Fundación CEDDET. Ob. Cit. Página 34.

Tanto en el derecho español como en el uruguayo el consentimiento ha de ser por definición informado, en el momento de la recogida directa de los datos habrá que cumplir, con carácter previo, con el requisito de la información. Este derecho puede ser también cumplimentado por medio de cuestionarios u otros impresos.

Cuando el contenido de ella se deduzca claramente de la naturaleza de los datos solicitados o de las circunstancias de la recogida, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, cuando al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. El artículo 24.1 también prevé la excepción cuando la información al afectado afecte la Defensa Nacional, a la Seguridad Pública o a la persecución de infracciones penales o administrativas.

Según Emilio del Peso el deber de información, junto al deber de obtención del consentimiento, son los dos principios sobre los que se construye el edificio de la protección de datos de carácter personal. El deber de información ha sido definido por parte de la doctrina como derecho de conocimiento por parte del interesado. El derecho a la información en la recogida de datos se encuentra regulado en el artículo 5 de la LOPD[13].

En el caso español, la cláusula informativa debe contener como mínimo, lo siguiente: existencia de un fichero, finalidad para la que se recaban, destinatario de los datos e identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

La AEPD resolvió un expediente de denuncia (PS/00098/2009) en el que se declaraba que se había recibido publicidad no solicitada por la empresa FINGES SA, en la que no constaba dirección alguna para ejercer los derechos que le reconoce la Ley orgánica 15/1999. La Agencia resolvió sancionar a la entidad por infracción del artículo 5 de la LOPD, considerando que el tratamiento de datos por parte de la empresa carecía de la información previa necesaria[14].

6. Principio de seguridad de los datos

El artículo 10 de la ley uruguaya establece el Principio de seguridad de los datos, estableciendo que el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas

[13]DEL PESO NAVARRO Emilio, RAMOS GONZALEZ Miguel Angel, DEL PESO RUIZ Margarita y DEL PESO RUIZ Mar. *Nuevo reglamento de protección de datos de carácter personal. Medidas de Seguridad*. Ediciones Díaz de Santos. 2008. Página 77.

[14] www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2009/index-ides-idphp.php

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.

En el inciso final establece la prohibición de registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.

El decreto reglamentario en sus artículos 7 y 8, inspirados en el documento borrador de los Estándares Internacionales de protección de datos, que fueran aprobados en la 31º Conferencia Internacional de Protección de Datos de Madrid en noviembre de 2009, establece lo siguiente:

"Artículo 7º. Medidas de seguridad. Tanto 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.

Artículo 8º. Vulneración de seguridad. Cuando 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".

Respecto a este tema, señala el Dr. Rebollo que: "La seguridad incumbe al responsable del tratamiento o, en su caso, al encargado del mismo, y se cumplimenta con la adopción de medidas técnicas y organizativas para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado. Las medidas a adoptar dependen, según el precepto, "del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural". La seguridad abarca tres conceptos: la confidencialidad, la integridad y la disponibilidad"[15].

Es de destacar que, a diferencia de la ley uruguaya, en la normativa española existen tres niveles de medidas de seguridad: básico, medio y alto, las que se encuentran reguladas en el Real Decreto 1720/2007[16]:

Nivel básico: todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad de nivel básico.

Nivel medio: los ficheros o tratamientos de datos de carácter personal que contengan datos relativos a la comisión de infracciones administrativas o

[15] Rebollo Delgado, L y Serrano Pérez M: *Introducción a la protección de datos*. Ob. Cit.
[16] Protección de Datos para Universidades. APDCM, 2008. Páginas 462 y 263.

penales; aquellos cuyo funcionamiento se rija por el Artículo 29 de la LOPD (prestación de servicios de información sobre solvencia patrimonial y crédito); aquellos de los que sean responsables Administraciones tributarias y se relacionan con el ejercicio de sus potestades tributarias, aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros; aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias; aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; y aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o comportamiento del individuo.

Nivel alto: los ficheros o tratamientos de datos de carácter personal que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual; los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas; y los que contengan datos derivados de actos de violencia de género.

El Real Decreto plantea dos excepciones a las medidas de seguridad de nivel algo, que son:

1. los ficheros que contengan datos relativos a la ideología, afiliación sindical, religión o creencias, así como a la salud, cuya finalidad sea únicamente la transferencia dineraria a las entidades de las que los afectados sean asociados o miembros o se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria contengan datos sin guardar relación con su finalidad;

2. los ficheros que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos (por ejemplo, un fichero de nóminas). En estos casos de deberán adoptar medidas de seguridad de nivel básico.

Pero también, el Real Decreto especifica las medidas de seguridad de los ficheros informatizados:

- Artículos 89 a 94, regulan las de nivel básico (Documento de seguridad; funciones y obligaciones del personal; registro de incidencias; control de acceso; gestión de soportes y documentos; identificación y autentificación; copias de respaldo y recuperación).

- Artículos 95 a 100, las de nivel medio (Responsable de Seguridad; auditoría; gestión de soportes y documentos; identificación y autentificación; control de acceso físico; registro de incidencias).

- Artículos 101 a 104, las de nivel alto (gestión y distribución de soportes, copias de respaldo y recuperación; registro de accesos; telecomunicaciones).

Una de las principales novedades del Decreto es que regula, por primera vez, ficheros no automatizados (manuales). Se ha seguido algunas medidas de seguridad contenidas en Recomendaciones de la Agencia de Protección de Datos de la Comunidad de Madrid:

- Recomendación 2/2004 de 30 de julio sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas, y

- Recomendación 1/2005 de 5 de agosto sobre Archivo, Uso y Custodia de la Documentación que compone la Historia Social no informatizada por parte de los Centros Públicos de Servicios Sociales de la Comunidad de Madrid.

Por otra parte, establece medidas de seguridad "genéricas" de los ficheros automatizados que resulten de aplicación a los ficheros no automatizados, como por ejemplo el documento de seguridad.

Existen, a su vez, tres criterios específicos para la adopción de medidas de seguridad de ficheros no automatizados:

- Los criterios referentes al archivo, con una referencia a la legislación aplicable en esta materia que será relativa a la normativa que regula los archivos.

- Los referentes a los dispositivos de almacenamiento, que deberán disponer de mecanismos que obstaculicen su apertura.

- Los referentes a la custodia de soportes, por los cuales las personas encargadas de la custodia, mientras que la documentación en formato papel esté en proceso de revisión o tramitación, deberá vigilarla e impedir que cualquier persona no autorizada pueda acceder a ella.

7. Principio de reserva

En la Ley Nº 18.331 se regula el Principio de reserva en el artículo 11, el cual establece que: ***"****Aquellas 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.*

Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular.

Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos".

En el derecho español encontramos regulado el deber de secreto en el artículo 10 de la LOPD, que establece que incumbe al responsable del fichero y a todas las personas que participan en cualquier fase del tratamiento y afecta a los datos de carácter personal conocidos durante su relación laboral con el fichero. El secreto sobre los datos debe prolongarse incluso después de finalizar las relaciones con el titular del fichero o su responsable.

No debe confundirse este deber de secreto con el secreto profesional al que están sometidas determinadas personas en función de la profesión que ejercen. Este deber de secreto es un deber genérico que alcanza a cualquier persona que intervenga en el tratamiento de los datos. Sin embargo, la ley uruguaya, en algunos casos lo equipara al secreto profesional, sobre todo a la hora de regular su sanción.

La Agencia de Protección de Datos de la Comunidad de Madrid recomienda[17]: la inclusión de cláusulas específicas en esta materia en los contratos laborales que suscriban las Administraciones Públicas de su ámbito de actuación con empleados públicos, cuyo texto se encuentra disponible en www.apdcm.es Canal Servicios.

8. Principio de responsabilidad

En este caso, el artículo 12 de la ley uruguaya es muy sencillo, estableciendo simplemente que el responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley.

El documento de Estándares Internacionales establece bajo este principio que: "*La persona responsable deberá:*

a. *Adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable, y*

[17] Protección de Datos para Universidades. APDCM, 2008. Página 465.

b. *Dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23".*

9. Principio de transparencia

Se encuentra enunciado en la Resolución de Madrid sobre Estándares Internacionales y se desarrolla en seis puntos:

1. Toda persona responsable deberá contar con políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere.

2. La persona responsable deberá facilitar a los interesados información sobre su identidad, de la finalidad del tratamiento, de los destinatarios a los que prevé ceder los datos y de la forma que los interesados podrán ejercer los derechos.

3. Cuando los datos de carácter personal hayan sido obtenido directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitado con anterioridad.

4. Cuando los datos personales no hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en un plazo prudencial de tiempo, si bien podrá sustituirse por medidas alternativas cuando su cumplimiento resulte imposible o exija un esfuerzo desproporcionados a la persona responsable.

5. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad.

6. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos.

10. Conclusiones

Sin lugar a dudas los principios generales son la base de la interpretación y aplicación de la normativa de protección de datos, constituyéndose en la brújula que guía el actuar de los responsables, garantiza la efectiva

aplicación del derecho a los ciudadanos y orientan las decisiones de los órganos de control.

Además de los principios analizados, recogidos en la ley uruguaya bajo el nomen iuris respectivo, también se desprenden de estos artículos otros principios, como el de proporcionalidad, en virtud a que el artículo 7 establece que los datos que se recogieren deberán ser “no excesivos”. Por otra parte en el artículo 7 se recoge el principio de exactitud, cuando establece que los datos deben ser exactos y actualizarse en el caso en que ello fuere necesario y cuando se constate la inexactitud o falsedad de los datos. Asimismo, en el artículo 8 al referirse al principio de finalidad, regula en el inciso 2 la conservación de los datos, al establecer que los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados.

Del análisis realizado surge que los principios son denominados de manera diferente, pero que con pequeñas variantes el énfasis está puesto en los mismos aspectos. Por otra parte, podemos concluir también que la normativa uruguaya está alineada a la normativa europea y a los postulados de la doctrina en el tema.

BIBLIOGRAFIA

Cuaderno informativo sobre protección de datos. APDCM, 2002.

Del Peso Navarro E., Ramos González M., Del Peso Ruiz M. y Del Peso Ruiz M. *Nuevo reglamento de protección de datos de carácter personal. Medidas de Seguridad*. Ediciones Díaz de Santos. 2008.

Delpiazzo C. y Viega MJ. *Lecciones de Derecho Telemático. Tomo I*. Fundación de Cultura Universitaria, abril 2004.

Delpiazzo C. y Viega MJ. *Lecciones de Derecho Telemático. Tomo II*. Fundación de Cultura Universitaria, marzo 2009.

Directrices de la OCDE.

Directrices para la armonización de la protección de datos en la comunidad iberoamericana. Red Iberoamericana de Protección de Datos, Cartagena de Indias a 4 de Mayo de 2007

El acceso a la información pública y la protección de los datos personales. Huixquilucan (Estado de México), 4 de noviembre de 2005.

Estándares Internacionales sobre Protección de datos personales y privacidad. Resolución de Madrid, 5 de noviembre de 2009.

Estudio sobre Protección de Datos a nivel internacional. IFAI, noviembre 2004.

López Calvo, J., García Prieto, M., Navarro Alonso I. y Lobato Lobato Angelina. *Módulo 2. Principios básicos de la protección de Datos*. Curso "El derechos a la protección de datos personales, 1º edición. Fundación CEDDET.

Murillo de la Cueva P. y Piñar Mañas JL. *El derecho a la autodeterminación informativa*. Fundación Coloquio Jurídico Europeo. Madrid, 2009.

Protección de Datos para Universidades. APDCM, 2008.

Real, AR. *Los principios generales de Derecho en la Constitución uruguaya*. Montevideo, 1965.

Rebollo Delgado, L y Serrano Pérez M: *Introducción a la protección de datos*. 2ª Ed. Madrid 2008.