Resoluciones dictámenes e informes

2009

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY

agesic
agencia de gobierno electrónico
y sociedad de la información

INDICE

PRÓLOGO

La ley No. 18.331 de 11 de agosto de 2008 reconoce el derecho a la protección de datos personales como inherente a la personalidad humana y, por lo mismo, comprendido en el art. 72 de la Constitución de la República.

Refiere al contenido de ese derecho, prevé procedimientos administrativos y jurisdiccionales para su garantía, desarrolla los principios que regulan la materia y, en general, establece un régimen de tutela de los datos personales de manera acorde a un Estado personalista de Derecho de comienzos del siglo XXI, en el cual las técnicas de información que contribuyen a una mejor vida humana, pueden –a la vez – incidir negativamente en ella, en este caso en lo atinente a datos propios de cada persona.

Por lo expuesto, es con satisfacción que el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP) creada por la citada ley –que funciona desde fines de mayo de 2009 – presenta la publicación Resoluciones, Dictámenes e Informes URCDP 2009.

Dicho Consejo está integrado por el Ing. José Clastornik, Director ejecutivo de AGESIC; el Mag. Federico Monteverde y quien escribe estas líneas; y cuenta, además, con el apoyo técnico de personal de esa Agencia, en especial de su Dirección de Derechos Ciudadanos, a cuyo frente se encuentra la Dra. María José Viega Rodríguez.

La publicación contiene resoluciones y dictámenes del Consejo, así como informes emitidos por la Dra.Flavia Baladán, el Dr. Marcelo Bauzá, el Dr.Federico Carnikián y la Dra. María José Rodríguez Tadeo.

Los documentos incluidos permiten apreciar la diversidad de cuestiones consideradas en el ámbito de la Unidad, así como su relevancia conceptual y práctica en la aplicación de las reglas de derecho que regulan los datos personales y su protección, en cuyo cumplimiento estamos todos involucrados, dado su indudable interés general.

En la página Web de la URCDP (www.datospersonales.gub.uy), se dio publicidad a documentación de la misma (resoluciones y dictámenes), así como otras informaciones relacionadas.

Se ha estimado, de todas maneras, que resulta de interés la edición por esta otra vía, en virtud del referido interés general de los temas y el elevado nivel técnico de los informes producidos por los profesionales ya mencionados.

Dr. Felipe Rotondo Tornaría

Resolución N° 17 de 12 de junio de 2009.- Se resuelve sobre los países que no requieren autorización de la Unidad Reguladora y de Control de Datos Personales para realizar transferencias internacionales de datos

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Montevideo, 12 de junio de 2009

VISTO:

La necesidad de poner en conocimiento cuáles son los países que no requieren autorización de la Unidad Reguladora y de Control de Datos Personales (URCDP) para la transferencia internacional de datos personales, conforme lo dispuesto por el artículo 23 de la Ley Nº 18.331 de Protección de Datos Personales y Acción de Habeas Data (LPDP).

RESULTANDO:

I) Que la transferencia internacional de datos en tanto tratamiento de datos que supone una transmisión de éstos fuera del territorio nacional, constituye una cesión o comunicación que tiene por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo.

II) Que a efectos de brindar lineamientos claros para la solicitud de transferencias internacionales promovida por el exportador que pretenda llevarla a cabo, resulta necesario delimitar en qué casos no es requerida la autorización por parte de la URCDP.

CONSIDERANDO:

I) Que el artículo 23 de la LPDP regula la transferencia internacional de datos personales, disponiendo su prohibición con países u organismos internacionales que no proporcionen niveles de protección adecuados, de acuerdo con los estándares del Derecho Internacional o Regional en la materia, salvo las excepciones allí enumeradas.

II) Que 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, prevé en su artículo 25, apartado 1, que los Estados miembros de la Unión

Europea sólo permitirán la transferencia de datos personales a un tercer país si éste proporciona un nivel de protección adecuado y se cumplen en él, con anterioridad a la transferencia, las disposiciones que los Estados miembros aprueben en aplicación de otros preceptos de dicha Directiva.

III) Que la Comisión Europea puede determinar que un tercer país garantiza un nivel de protección adecuado, habilitándose en ese caso la transferencia de datos personales desde los Estados miembros sin que sea necesario ninguna garantía adicional.

IV) De acuerdo a la Directiva 95/46/CE, el nivel de protección de los datos debe evaluarse atendiendo a todas las circunstancias que concurran en una transferencia o conjunto de transferencias de datos y evaluando una serie de elementos relevantes para la transferencia, enumerados en el apartado 2 de su artículo 25.

ATENTO:

A lo precedentemente expuesto y a lo establecido por el artículo 23 de la Ley Nº 18.331 de Protección de Datos Personales y Acción de Habeas Data y disposiciones citadas de la Directiva 95/46/CE, el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1) Establecer que se consideran países apropiados para las transferencias internacionales de datos, aquellos que a juicio de esta Unidad, cuenten con normas de protección adecuadas y medios para asegurar su aplicación eficaz.

2) Declarar que en virtud de lo establecido en el numeral precedente, se encuentran comprendidos los países miembros de la Unión Europea y aquellos que la Comisión Europea considere garantizan las condiciones antes indicadas, en base a la normativa citada en la presente resolución.

Firmado por A/P Federico Monteverde
Ing. José Clastornik
Dr. Felipe Rotondo

Resolución N° 25 de 17 de julio de 2009.- Se resuelve denuncia por inclusión en la base de datos "Central de Riesgos Crediticios" del Banco Central del Uruguay

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Montevideo, 17 de julio de 2009

VISTO:

La denuncia presentada ante la Unidad por inclusión de datos personales en la base de datos "Central de Riesgos Crediticios del Banco Central del Uruguay – CRC".

RESULTANDO:

I) Que el relato y antecedentes documentales aportados por el denunciante surge que su persona fue registrada en dicha base de datos en calidad de deudor de comisiones por valor de U$S 880,oo (dólares americanos ochocientos ochenta), a partir del cierre de su cuenta bancaria en la Sucursal Maldonado del Banco de la República Oriental del Uruguay, cierre que se produjo en el año 1998.

II) Que luego de la vista y comparecencia del denunciado, compulsadas que fueran las versiones y probanzas aportadas por ambas partes, surge de autos que efectivamente los datos registrados adolecieron de falta de veracidad (art. 7 de la Ley No. 18.331), no observaron las formas requeridas para la renovación temporal de su registro extendiéndose éste por tiempo mayor al permitido por la ley (art. 22 de la Ley No. 18.381), y no fueron eliminados en el plazo legal dispuesto para ello (art. 15 de la Ley No. 18.381).

CONSIDERANDO:

I) Que en su comparecencia el Banco Central del Uruguay aportó explicaciones sobre la demora experimentada para cancelar las anotaciones impugnadas, al tiempo que acreditó haberlo hecho finalmente.

II) Que está en curso el plazo legal de adecuación de las bases de datos a la Ley N° 18.331 publicada en D.O el 18 de agosto de 2008, N° 27549, el que fuera fijado en un año a partir de su entrada en vigor conforme el art. 46 del texto normativo.

ATENTO:

A lo precedentemente expuesto, el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

Hacer saber que:

1) En circunstancias como la presente, cuando una persona solicite acceso, rectificación, actualización, inclusión o supresión de sus datos personales contenidos en la base de datos "Central de Riesgos Crediticios – CRC" que lleva el Banco Central del Uruguay, se deberá cumplir con los arts. 14 y 15 de la Ley No. 18.331.

2) Corresponde a derecho que el Banco Central del Uruguay regularice la situación de la base de datos "Central de Riesgos Crediticios – CRC" de acuerdo a la Ley No. 18.331.

Firmado por A/P Federico Monteverde
Ing. José Clastornik
Dr. Felipe Rotondo

Resolución N° 68 de 23 de octubre de 2009.- Se resuelve sobre denuncia por vulneración de datos personales en virtud de una comunicación de datos sin consentimiento

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Montevideo, 23 de octubre de 2009

VISTO:

La denuncia presentada por la Sra. AA poniendo en conocimiento de la Unidad Reguladora y de Control de Datos Personales (URCDP) una eventual vulneración de sus datos personales.

RESULTANDO:

I) Que AA expresa que realizó una compra a la empresa BB. Relata que a la semana siguiente se comunicaron telefónicamente con ella de la empresa CC ofreciéndole un seguro especial como beneficio derivado de la compra realizada en la primera empresa mencionada.
Expresa que los datos que poseía la empresa consistían en su nombre, teléfono celular, tarjeta de crédito y datos consignados en la boleta de su compra.

II) Que la empresa BB evacúa en tiempo y forma la vista conferida, expresando "Que a fin de incentivar las ventas, es política de BB realizar promociones y sorteos de productos propios o de terceras empresas, invitando a participar en las mismos a aquellos compradores de DD que lo deseen" y "Al tomar conocimiento de la denuncia en vista, procuramos la documentación correspondiente a este consentimiento. Sin embargo, por motivos que desconocemos, advertimos que en este caso particular no se habría recabado dicho consentimiento (...)". (fs. 12)

III) Que se le dio traslado a la denunciante de los descargos formulados por BB y habiendo transcurrido el plazo correspondiente no se presentó a evacuarlo. (fs. 14 a 15 vto.).

CONSIDERANDO:

I) Que de acuerdo a lo preceptuado en el artículo 4º de la Ley Nº 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP) se entiende por dato personal "i*nformación de cualquier tipo referida*

a personas físicas o jurídicas determinadas o determinables" y por tratamiento de datos personales "*operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias*" (literales D y M respectivamente). Asimismo, se define a la comunicación de datos como "*toda revelación de datos realizada a una persona distinta del titular de los datos*" (literal b).

II) Que se verifica una situación de comunicación de datos personales y que para poder realizarla es necesario contar con el consentimiento informado del titular de los datos.

III) Que el art. 9 literal c) preceptúa que respecto a las personas físicas no es necesario recabar el consentimiento respecto a su nombre y apellido, documento de identidad, nacionalidad, domicilio y fecha de nacimiento.

IV) Que no se constata la existencia de un contrato entre la empresa BB y CC que se exima de la necesidad de consentimiento y que asimismo no se consideran aplicables ninguna de las otras aplicaciones consignadas en el art. 9 de la LPDP.

V) Que el art. 8 de la LPDP, que regula el principio de finalidad, establece que los datos personales no deben utilizarse para una finalidad distinta o incompatible para la que fueron recabados.

VI) Que la URCDP puede aplicar medidas sancionatorias a quienes infrinjan las disposiciones de la LPDP, conforme lo prevé el artículo 35.
De las consideraciones realizadas surge acreditada la vulneración a las disposiciones de la LPDP, en tanto se violentaron los principios de previo consentimiento informado y de finalidad. Por tanto, por no revestir el carácter de grave, corresponde imponer la sanción de apercibimiento.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas, el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1) Imponer a la empresa BB la sanción de apercibimiento por la infracción a los artículos 8 y 9 de la LPDP, de conformidad con lo dispuesto por el artículo 35 numeral 1^{0} de la Ley citada.

2) Notifíquese, publíquese y oportunamente archívese.

Firmado por A/P Federico Monteverde

Resolución N° 74 de 4 de diciembre de 2009.- Se resuelve sobre denuncia por envío de mensajes de texto sin consentimiento

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Montevideo, 4 de diciembre de 2009

VISTO:

La denuncia presentada por el Sr. AA ante la Unidad Reguladora y de Control de Datos Personales (URCDP) por envío de mensajes de textos sin consentimiento por parte de la Administración Nacional de Telecomunicaciones (ANTEL).

RESULTANDO:

I) Que el 3 de setiembre de 2009 se presentó AA ante la URCDP manifestando a fs. 1 que cuando ANCEL había empezado a enviar mensajes de texto ofreciendo diferentes productos había solicitado la baja y se había procedido a realizar ésta.
En el transcurso del presente año comenzó a recibir nuevas comunicaciones, especificando las fechas, siendo estas sin su consentimiento.

II) Que el 8 de setiembre de 2009 se confirió vista a ANTEL, la que fue evacuada el 29 de setiembre de 2009. A fs. 17 y 17 vuelto manifiesta que en algunas oportunidades ANTEL realiza envío de comunicaciones a sus clientes, que posee una lista negativa de personas que no quieren recibir estas, que no tienen un histórico tan antiguo, que imputa el error a un problema informático y que se ha procedido a inclusión para no recibir más mensajes.

III) Que a fs. 21-22 se produjo el informe jurídico correspondiente.

CONSIDERANDO:

I) Que para el tratamiento de datos personales por parte del responsable de una Base de Datos sea lícito, aún cuando la finalidad sea la de enviar comunicaciones comerciales o publicitarias por vía electrónica, se requiere como regla general, el consentimiento del titular de los datos, el que deberá ser pre-

vio, expreso, informado y además deberá documentarse, conforme lo prevé el artículo 9° de la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP). La mencionada disposición establece excepciones, las que no resultan aplicables en la especie.

II) Que el artículo 15 de la LPDP otorga a toda persona física o jurídica el derecho a solicitar la supresión de los datos personales que le corresponda, incluidos en una Base de Datos, al constatarse error en su inclusión.

III) Que el artículo 21 regula las Bases de Datos con fines de publicidad, estableciendo que podrán ser tratados cuando hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. Asimismo, establece que el titular podrá en cualquier momento solicitar el retiro de sus datos de la mencionada Base de Datos.

IV) Que surge probado en el presente expediente, que fue admitido por el propio denunciado, ANTEL infringió los artículos referidos en tanto no suprimió los datos personales de AA pese a la solicitud de éste.

V) Que la URCDP, de acuerdo a lo previsto en el artículo 35 de la LPDP podrá aplicar medidas sancionatorias a los responsables de las Bases de Datos cuando violen las disposiciones de la LPDP.

ATENTO:

A lo expuesto, al informe glosado en fs. 21-22 y a lo previsto en las normas legales citadas, el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1) Imponer a ANTEL la sanción de apercibimiento por la infracción a los artículos 15 y 21 inciso final de la LPDP, de conformidad con lo dispuesto por el artículo 35 numeral 1° de la Ley citada.

2) Notifíquese, publíquese y oportunamente archívese.

Firmado por A/P Federico Monteverde
f.b.

Resolución N° 129 de 17 de diciembre de 2009.- Se resuelve sobre denuncia por una oferta comercial comunicada a través de correos electrónicos masivos

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Montevideo, 17 de diciembre de 2009

VISTO:

Las actuaciones cumplidas en el expediente a propósito de la oferta comercial denominada "DIRECTORIO DE 4.500 EMPRESAS URUGUAYAS" comunicada a través de correos electrónicos masivos.

RESULTANDO:

I) Que de conformidad con la Resolución Nº 62 del 02-10-2009 dictada previamente en el expediente, se recibieron descargos de parte del Sr. AA, quien se presentara como titular de dicho Directorio y único promotor de la actividad realizada.

II) Que si bien no se comparten totalmente las apreciaciones del compareciente, las mismas se aceptarán parcialmente en consonancia a lo expuesto en el Informe Letrado Nº 98 dictado en autos el 22 de octubre de 2009 al que este Consejo se remite *brevitatis causae*.

CONSIDERANDO:

I) Que es competencia de esta Unidad, controlar la observancia del régimen constitucional y legal de la protección de datos personales, en ejercicio de los cometidos legales que le impone el Artículo 34 acápite y literal D) de la Ley Nº 18.331 de 11-08-2008.

II) Que surgen del expediente apartamientos a los Artículos 6º, 9º y 17º de la Ley Nº 18.331.

III) Que en función de la primariedad, y de la formal declaración del compareciente en cuanto a que destruyó el objeto en infracción y ya no dispone del mismo, corresponde aplicar la medida sancionatoria preceptuada en el Artículo 35, numeral 1) de la Ley Nº 18.331, con la advertencia del caso.

ATENTO:

A lo precedentemente expuesto, y a lo informado por la vía letrada el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1) Establecer que el Sr. AA no ha cumplido con el régimen jurídico de protección de datos personales, al haber ofrecido comercialmente mediante correos electrónicos masivos, un directorio conteniendo información de empresas uruguayas.

2) Adviértase a la misma persona que en el futuro deberá ajustar su conducta particular y/o de quienes represente, en materia de publicidad y ofertas comerciales, a los preceptos legales vigentes, en especial a las Leyes Nros. 17.250 y 18.331, bajo prevención de imponérsele sanción mayor si no lo hiciere.

3) Notifíquese, publíquese y archívese.

Firmado por A/P Federico Monteverde

Resolución N° 174 de 23 de diciembre de 2009.- Se resuelve sobre consulta referida a si los sujetos regulados por el Banco Central del Uruguay deben registrar sus bases de datos, así como si corresponde documentar el consentimiento de sus clientes

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Montevideo, 23 de diciembre de 2009

VISTO:

La consulta recibida referente a si los sujetos regulados por el Banco Central del Uruguay deben registrar sus Bases de Datos, y si corresponde documentar el consentimiento de sus clientes.

RESULTANDO:

I) Que la consultante entiende que no procede el registro de estas bases de datos ni documentar el consentimiento de los clientes.

II) Que no es compartible la primera apreciación, y sí en cambio lo es la segunda, todo ello por remisión extensiva a las consideraciones y fundamentos que surgen del informe jurídico de autos, cuyos lineamientos principales se exponen a continuación.

CONSIDERANDO:

I) Que la Ley Nº 18.331 de 11 de Agosto de 2008 configura el régimen legal general en el derecho positivo uruguayo actual, en materia de protección de datos personales, en tanto derecho inherente a la persona humana comprendido dentro del art. 72 de la Constitución de la República (art. 1º de la Ley).

II) Que para excepcionar de este régimen en aplicación del art. 3 inc. 3 lit. C del mismo cuerpo normativo, debe existir un dispositivo regulador garantista igual o superior al que pretende exceptuarse, o bien otro tipo de intereses de consideración superior que permitan sobrepujar el derecho de la protección de datos personales, situaciones que no acaecen en la hipótesis sometida a consulta.

III) Que ni la Ley Nº 17.948 de 8 de enero de 2006 (información bancocentralista), ni la Ley Nº 16.696 de 30 de marzo de 1995 con las modificaciones introducidas por la Ley Nº 18.401 de 24 de octubre de 2008 (Carta Orgánica del BCU),

aportan elementos "reguladores" garantistas del tenor requeridos, como tampoco lo hacen las disposiciones administrativas dictadas hasta el presente en ejercicio de la potestad reglamentaria del Ente en materia de información requerida a las entidades de intermediación financiera.

IV) Que dada la novel experiencia de nuestro sistema jurídico en la materia, resulta oportuno acudir al ejemplo de quienes poseen larga tradición en estos temas, a vía de ejemplo el derecho español, donde al fichero CIRBE del Banco de España, si bien con algunas particularidades que son igualmente de origen legal, se le aplica el régimen de la Ley 15/99, o sea la ley orgánica de protección de datos personales española.

V) Que en materia de consentimiento de los titulares de datos personales, la Ley Nº 18.331 establece algunas posibilidades de excepción que procede aplicar a la especie, permitiendo prescindir de dicho consentimiento sin perjuicio de cumplir con el deber de información al titular al momento de recabar sus datos.

ATENTO:

A lo dispuesto por el art. 72 de la Constitución de la República; los arts. 1, 3, 6, 9 C y D, 13, 24, 28, 29 y 33 A) de la Ley Nº 18.331 de 11 de agosto de 2009; lo expuesto y el informe jurídico vertido a propósito de la consulta recibida, el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1) Declarar que los sujetos regulados por el Banco Central del Uruguay deben cumplir con la Ley Nº 18.331 de 11 de Agosto de 2009 en todos sus términos, incluyendo el registro de sus bases de datos ante esta Unidad.

2) Declarar que en tales casos, y en tanto se trate de alguna de las hipótesis de excepción previstas en el art. 9 de precitada Ley, los referidos sujetos podrán prescindir del consentimiento de los clientes que aporten sus datos a dichas bases, sin perjuicio de cumplir con el deber de información en los términos preceptuados en el art. 13 de la misma Ley.

Firmado por A/P Federico Monteverde

Dictamen N° 2 de 27 de abril de 2009.- Se dictamina sobre una consulta del Ministerio de Salud Pública, respecto a la posibilidad de publicar en su sitio web las demás actividades laborales declaradas por los inspectores de dicha Secretaría de Estado

Montevideo, 27 de abril de 2009

Dictamen N° 2
Exp. 2009/008
Ref.: Publicación en web de otras actividades laborales declaradas por Inspectores del M.S.P.

VISTO:

La consulta realizada por el Ministerio de Salud Pública (en adelante M.S.P.) de acuerdo a lo previsto en el articulo 34 literal g) de la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data (en adelante LPDP) referido a la posibilidad de publicar en la web las demás actividades laborales declaradas por los Inspectores de dicha Secretaría de Estado.

RESULTANDO:

I) Que el M.S.P. tiene la iniciativa de publicar las demás actividades laborales de los Inspectores del Ministerio a efectos de dar mayor transparencia en la gestión, teniendo en consideración no lesionar disposiciones legales.

II) Que corresponde emitir opinión por parte de la URCDP en todos los temas relacionados con la protección de datos.

III) Que con fecha 15 de abril de 2009 se elaboró el correspondiente Informe jurídico.

CONSIDERANDO:

I) Que la situación planteada refiere a aspectos relacionados con la necesidad o no del previo consentimiento para su publicación, y si se verifican las excepciones contenidas en los literales B), C) y D) del art. 9 de la LPDP.

II) En cuanto al literal B) tomando en consideración la amplitud de los cometidos que pueden tener esa Secretaría de Estado y que en la situación de marras lo que se busca es lograr la mayor transparencia en la gestión, podría entenderse que en el caso concreto es aplicable dicha excepción.

III) Que respecto a la excepción contenida en el literal C) se entiende que cons-

tituyen datos personales por lo que se requiere el previo consentimiento ya que la enumeración realizada es taxativa y no comprende dichos datos.

IV) Que en referencia al literal D) se podría considerar comprendida dentro de este artículo en tanto se considere que para el ejercicio de sus funciones del Ministerio es necesario comprobar la inexistencia de una actividad incompatible.

V) Que el caso conforma una comunicación de datos de acuerdo a lo previsto en el art. 17 de la Ley N° 18.331 y por tanto es necesario analizar la existencia de interés legítimo. Que respecto al interés del emisor se podría inferir que podría ser necesario a efectos de lograr la mayor transparencia en la gestión del Ministerio.

ATENTO:

A lo precedentemente expuesto y a lo dispuesto por los artículos 9°, 17 y 34 de la LPDP, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

Se sugiere publicar las demás actividades laborales de los Inspectores del M.S.P. en la medida que la mentada publicación forma parte de las funciones propias del Organismo y la finalidad perseguida es la mayor transparencia en la gestión. De lo contrario, será necesario recabar el previo consentimiento informado, de acuerdo a las previsiones contenidas en el art. 9° de la LPDP.

Firmado por A/P Federico Monteverde
Ing. José Clastornik
Dr. Felipe Rotondo

Dictamen N° 3 de 22 de mayo de 2009.- Se dictamina sobre una consulta de la Gerencia de Seguridad del Lloyds TSB Bank sobre la firma de cláusulas especiales de protección de datos para la transferencia internacional de datos

Montevideo, 22 de mayo de 2009

Dictamen Nº 3
Exp. 2009/013
Ref. Consulta sobre cláusulas especiales de contrato exigidas por la Cámara Internacional de Comercio

VISTO:

La consulta remitida por la Gerencia de Seguridad del Loyds TSB Bank ante la exigencia de un cliente, de la firma de cláusulas especiales de protección de datos para la transferencia de datos personales.

RESULTANDO:

I) Que la Gerencia de Seguridad del Lloyds TSB Bank solicita la opinión de la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP) como organismo especializado sobre el tema adjuntando a tales efectos la documentación correspondiente.

II) La consultante manifiesta estar en conocimiento de la Ley de Protección de Datos de la Unión Europea, del motivo por el cual el cliente les exige la firma de cláusulas especiales y de que Uruguay no tiene aun el reconocimiento de la UE como país adecuado para el intercambio de información de datos personales.

III) Que con fecha 5 de mayo de 2009 se elaboró el informe jurídico correspondiente.

CONSIDERANDO:

I) Que la URCDP tiene entre sus cometidos el de asistir y asesorar a las personas que lo requieran acerca de los alcances de la Ley de Protección de Datos Personales y Acción de Habeas Data Nº 18.331 (en adelante LPDP) y de los medios legales de que disponen para la defensa de los derechos que ella garantiza, conforme lo previsto por el literal a) de dicha disposición legal.

II) Si bien le asiste razón al consultante en el sentido que Uruguay aún no tiene el reconocimiento de la Unión Europea como país adecuado para el intercambio de información de datos personales, la adecuación se encuentra en trámite. Sin per-

juicio de ello, se encuentra vigente la LPDP desde el 11 de agosto de 2008; y en trámite de aprobación el Anteproyecto del Decreto Reglamentario de la Ley.

III) Hasta tanto la adecuación no se verifique, resulta legítimo que exportadores de datos de la Comunidad Europea propicien la implementación de cláusulas contractuales en las transferencias internacionales con aquellos importadores de datos de terceros países, conforme lo prevé la Directiva de la Unión Europea 95/46/CE relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

IV) La Cámara Internacional de Comercio ya ha presentado un conjunto alternativo de cláusulas contractuales tipo, pensado para ofrecer un nivel de protección de datos equivalente al proporcionado por el conjunto de cláusulas adoptado por la Decisión 2001/497/CD, aunque utilizando mecanismos diferentes.
(Considerando 2 de la Decisión de la Comisión 2004/915/CE de 27 de diciembre de 2004).

V) De un análisis preliminar de las cláusulas alternativas que se pretenden implementar, glosadas a fs. 3-4 del expediente, se extrae que básicamente consagran las garantías que brinda la Decisión de la Comisión de las Comunidades Europeas 2004/915/CE.

ATENTO:

A lo expuesto y lo dispuesto por los artículos 23, 34 literal a) de la Ley Nº 18.331; artículo 25 y 26 numeral 2º de la Directiva de la Unión Europea 95/46/CE, Decisión de la Comisión de las Comunidades Europeas 2004/915/CE, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido que la implementación de cláusulas como la presente, resulta favorable para el intercambio de información de datos personales entre exportadores de datos de la Comunidad Europea e importadores de datos de terceros países, en tanto ofrezcan niveles de protección que resulten en consonancia con los estándares internacionales (Directiva de la Unión Europea 95/46/CE y Decisión de la Comisión 2004/915/CE) y la normativa nacional vigente.

2) Hacer presente que aunque se adopten cláusulas especiales, en caso que Uruguay sea exportador de datos y el flujo de información lo sea con un tercer país que no garantice un nivel adecuado de protección, siempre se requerirá la autorización de la URCDP, conforme lo prevé la LPDP en su artículo 23.

Firmado por A/P Federico Monteverde
Ing. José Clastornik
Dr. Felipe Rotondo

Dictamen N° 4 de 22 de mayo de 2009.- Se dictamina sobre una consulta del diario "El País" sobre la legalidad de las llamadas realizadas con fines políticos

Montevideo, 22 de mayo de 2009

Dictamen Nº 4
Exp. 015/2009
Ref. Consulta sobre legalidad de las llamadas realizadas con fines políticos

VISTO:

Que llega a consideración de la Unidad Reguladora y de Control la consulta formulada por el Sr. Eduardo Delgado de la empresa periodística "El País" referente a la práctica de grupos políticos que están realizando publicidad telefónica de sus actividades.

RESULTANDO:

I) Que se trata de una práctica publicitaria constatada en nuestro medio, a partir de las campañas de candidatos a las elecciones internas de los partidos políticos.

II) Que la observancia de la Ley No. 18.331 en este punto depende de diferentes alternativas bajo las cuales la referida práctica se estuviere concretando en los hechos.

CONSIDERANDO:

I) Que al tenor del art. 4o. Literal E de la Ley, los números de teléfono celular y teléfono fijo de personas físicas o jurídicas, tienen la calidad de datos personales en tanto identifiquen, o puedan hacerlo, a sus titulares.

II) Que conforme el art. 9 de la Ley, debe exigirse la prestación de consentimiento libre, previo, expreso, informado y documentado del titular, a los efectos del tratamiento legítimo de sus datos; y en cuanto a la comunicación a terceros de dichos datos, el art. 17 de la Ley agrega -además del consentimiento- los requisitos de la información al titular sobre la finalidad de la comunicción y la identificación del destinatario (art. 17 de la Ley).

III) Que en caso de contar con el consentimiento directo del titular involucrado, el régimen legal establece de todos modos algunas excepciones a la regla, entre

las que figura que los datos objeto de tratamiento o comunicación posterior, provengan de fuentes públicas de información, fuente que indudablemente existe en materia de teléfonos fijos a través de la Guía Telefónica (siempre que el usuario no haya solicitad su exclusión), no así en materia de teléfonos celulares (art. 9 literal A de la Ley). Asimismo cabe considerar como excepción al régimen general del consentimiento del titular, la utilización de números telefónicos pertenecientes a personas jurídicas (art. 9 literal C de la Ley).

IV) Que en todo caso existe siempre la posibilidad de apelar al procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables (arts. 4 literal G, 17 literal D). Se menciona como ejemplo, la existencia de programas informáticos que permiten realizar llamados telefónicos en forma aleatoria, generando el número en forma randómica, lo que no constituye una base de datos.

ATENTO:

A lo consignado en el Informe Jurìdico que obra en autos y se comparte en plenitud, a lo expuesto en el presente acto, y a lo dispuesto por el artículo 34 literal A) de la Ley No. 18.331, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) En lo que respecta a la competencia de esta Unidad, cuando la difusión se realiza -en el caso de personas físicas- utilizando fuentes públicas de información como la Guía Telefónica, o bien se trata de números pertenecientes a personas jurídicas, dicha difusión resulta legítima.

2) En cualquier caso se considera lícita la posibilidad de disociación de la información de forma tal de volverla anónima, lo que puede hacerse mediante la utilización de listados que las empresas telefónicas cabe que suministren a terceros conteniendo exclusivamente números de teléfono, sin agregados ni conexiones con ninguna otra clase de datos que llevase a determinar los titulares de tales servicios. Sobre el punto, téngase presente, además, lo informado en el Considerando IV.

Firmado por A/P Federico Monteverde
Ing. José Clastornik
Dr. Felipe Rotondo

Dictamen N° 5 de 22 de mayo de 2009.- Se dictamina sobre una consulta de la Dirección Nacional de Catastro del Ministerio de Economía y Finanzas, referido a la adecuación del anteproyecto de ley catastral

Montevideo, 22 de mayo de 2009

Dictamen Nº 5
Exp. 11/2009
Ref. Consulta sobre Anteproyecto de Ley catastral

VISTO:

La consulta remitida por la Dirección Nacional de Catastro del Ministerio de Economía y Finanzas solicitando la evaluación del Anteproyecto de Ley Catastral que acompaña a tales efectos, a la luz del régimen jurídico consagrado por la Ley de Protección de Datos Personales No. 18.331.

RESULTANDO:

I) Que analizado el referido Anteproyecto de Ley, no se observan en su articulado conflictos o rispideces con el régimen de encuadre y control emergente de la mencionada Ley.

II) Que no obstante ello, se observan sí algunos puntos de confluencia entre ambas especies, aunque sin colisión expresa, y por tanto merecedores de reseña a simple título de sugerencias a tener en cuenta en la etapa de reglamentación y desenvoltura factual del régimen proyectado, una vez se apruebe el mismo.

III) Que dichos puntos refieren a:

1º) El contenido que podrían llegar a asumir los registros e informaciones recogidos, tratados y eventualmente suministrados nuevamente a terceros por la Dirección Nacional de Catastro, en función de los arts. 4 literales d, e, g, h, k, i, así como 8, 11,12, 13 y 16 del régimen proyectado.

2º) El cometido de "llevar y administrar el registro de los Profesionales habilitados para presentar documentación catastral ante la DNC" (art. 4 literal m del Anteproyecto de Ley en examen).

3º) El cometido de "aplicar sanciones a los Profesionales habilitados para presentar documentación catastral ante la Dirección Nacional de Catastro"

(art. 4 literal n del Anteproyecto de Ley en examen).

IV) Que con fecha 28 de Abril de 2009 se emitió el Informe jurídico correspondiente.

CONSIDERANDO:

I) Que resulta del caso aconsejar que los actos y actividades que pudiesen llegar a involucrar la recolección y tratamiento de datos por cualquier medio, electrónico o no electrónico, (ref. Resultando III 1o.), se reglamenten y, en definitiva, se lleven a cabo empleando criterios de restriccion y finalismo, cuando pudiesen involucrar datos personales (arts. 7 y 8 de la Ley 18.331).

II) Que a tales efectos resulta igualmente aconsejable tener presente el concepto amplio o progresivo de "dato personal" que permea todo el régimen (art. 4 literal d de la Ley 18.331), lo que obliga a tomar previsiones para preservar no solamente los datos de personas determinadas, sino además de personas "determinables".

III) Que por tales circunstancias será de buena práctica, en cuanto sea posible, proceder a la "disociación" de la información en los términos de los arts. 4 literal G y 17 inc. 3 literal D de la Ley 18.331, siempre que haya que recolectar y tratar datos que pudieran resultar pasibles de ser calificados, directa o indirectamente, como "dato personal".

IV) Que el art. 4 literal m del Anteproyecto de Ley alude (ref. al Resultando III 2o.), en este caso de modo directo, a un tipo de actividad como es "llevar y administrar un registro de Profesionales habilitados", que ingresa dentro del ámbito de la Ley 18.331. No juega aquí la excepción del art. 3 inc. 2 literal C de la Ley 18.331, en función de la triple exigencia conjunta emergente de la precitada norma, de interpretación estricta (creación, regulación, y por ley especial, de la base de datos que se trate), requisito que no se cumple en la especie.

V) Que el art. 4 literal n del Anteproyecto de Ley en examen remite, finalmente, (ref. a Resultando III 3o.) a ciertos actos que también ingresan dentro del ámbito de la Ley 18.331, y en este caso haciéndo una remisión a texto expreso a la reglamentación posterior, la que -por fundamentos similares a los que vienen de exponerse- deberá atenerse en un todo a las previsiones de la Ley 18.331.

ATENTO:

A lo expuesto y lo dispuesto por los artículos 4 literales D y G, 5 y ss. en especial

7 y 8, 17 inciso 3 literal D, 34 literal f) de la Ley Nº 18.331, la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1) Expedirse en el sentido de que el Anteproyecto de Ley consultado no vulnera las disposiciones de la Ley Nº 18.331.
2) Recomendar que la reglamentación, instructivos, manuales de funcionamiento, y en definitiva la operativa factual que acarree el régimen legal proyectado una vez aprobado, utilice conceptos y criterios tendientes a que los actos que refieran a la recolección y/o el tratamiento de datos, por cualquier medio o soporte (electrónico o no electrónico), cumplan con el régimen jurídico de protección de datos personales, con arreglo a las exigencias de la normativa vigente, y las sugerencias aportadas en el presente dictamen.

Firmado por A/P Federico Monteverde
Ing. José Clastornik
Dr. Felipe Rotondo

Dictamen N° 6 de 17 de junio de 2009.- Se dictamina sobre consulta referida a comunicación de datos entre la Dirección Nacional de Pequeñas y Medianas Empresas del Ministerio de Industria, Energía y Minería y la Dirección General Impositiva del Ministerio de Economía y Finanzas

Montevideo, 17 de junio de 2009

Dictamen Nº 6
Exp. 12/2009
Ref. Consulta sobre comunicación de datos de DGI a Dinapyme

VISTO:

Que llega a la consideración de esta Unidad Reguladora y de Control la consulta planteada por AA, sobre si DINAPYME (Ministerio de Industria y Energía) puede solicitar a la Dirección General Impositiva (Ministerio de Economía y Finanzas), los rangos de facturación y cantidad de empleados de las empresas, a partir del RUT de éstas.

RESULTANDO:

I) Que se han apreciado las especificaciones de la consulta, en cuanto a que la información solicitada excluiría montos facturados y número exacto de empleados, su justificación por la necesidad de contar con la misma para cumplir los cometidos de la DINAPYME, y que la DINAPYME no hará uso ni difusión de la información así obtenida, entre las Pymes.

II) Que con fecha 30 de Abril de 2009 se emitió el Informe jurídico correspondiente.

CONSIDERANDO:

I) Que la información cuya comunicación se pretende encuadra en el art. 17 de la Ley No. 18.331, que remite al art. 9 de la misma Ley, donde se establece que "no será necesario el previo consentimiento cuando...B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".

II) Que para el caso en consulta se trata de informaciones que constituyen un insumo imprescindible para cumplir con las funciones que la ley le asigna a la Dirección Nacional de Artesanías, Pequeñas y Medianas Empresas (DINAPYME), y que están preceptuadas en el art. 3 lit. C de la Ley 16.201, Ley No. 16.622 y art. 46 de la Ley No. 18.362.

III) Que del punto de vista del régimen jurídico dela protección de datos personales no existen impedimentos para dar curso a dicha transmisión de datos, en los términos establecidos en la consulta y el resto de la preceptiva legal, en especial el principio de reserva (art. 10 de la Ley No. 18.331) y el principio de finalidad en materia de comunicación de datos (art. 17 primera parte de la Ley No. 18.331).

ATENTO:

A lo expuesto, y a lo dispuesto por las disposiciones citadas y el art. 34 literal F de la Ley No. 18.331 la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

Declarar que la solicitud de la información aludida en la consulta, por parte de la Dirección Nacional de Artesanías y Pequeñas y Medianas Empresas (DINAPYME) dependiente del Ministerio de Industrias y Energía, a la Dirección General Impositiva (DGI) dependiente del Ministerio de Economía y Finanzas, no se opone a la Ley No. 18.331.

Firmado por A/P Federico Monteverde
Ing. José Clastornik
Dr. Felipe Rotondo

Dictamen N° 7 de 7 de agosto de 2009.- Se dictamina sobre una consulta de la Junta Departamental de Maldonado sobre la información que debe publicarse en su sitio web referido a expedientes que contienen datos personales

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Montevideo, 7 de agosto de 2009

VISTO:

La consulta de fs. 1 realizada por la Junta Departamental de Maldonado a la Unidad Reguladora y de Control de Datos Personales (URCDP).

RESULTANDO:

I) Que el 27 de julio de 2009 se presentó la Junta Departamental de Maldonado solicitando la opinión de esta Unidad.

II) Que la Junta Departamental de Maldonado expresa que ha recibido solicitudes de residentes del Departamento que consideran que la publicación en la página web de expedientes que contienen datos personales podría violar su intimidad o ser utilizados con fines delictivos y se solicita que se eliminen los datos personales consignados en los expedientes.

III) Que a fs. 52 y 52 vuelto se pronunció el asesor letrado de la Junta Departamental de Maldonado aconsejando solicitar la opinión de la URCDP.

IV) Que el 20 de julio de 2009 la Junta Departamental de Maldonado resolvió remitir las actuaciones a la URCDP.

V) Que con fecha 27 de julio de 2009 se remitió el expediente para informe jurídico, el cual fue elaborado el 31 de julio de 2009 (fs. 34- 35).

CONSIDERANDO:

I) Que de acuerdo a la definición contenida en el art. 4° de la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP), los expedientes de la Junta Departamental de Maldonado contienen datos personales.

II) Que respecto al tratamiento de datos personales se debe considerar el princi-

pio de finalidad contenido en el art. 8° de la LPDP, por el cual no se deben utilizar datos personales para una finalidad distinta para la que fueron recabados. No constando en dichos expedientes ninguna referencia a la publicación en la web de éstos.

III) Que de acuerdo al principio de proporcionalidad se considera desproporcionado publicar *in totum* los expedientes llevados por la Junta.

IV) Que se debe considerar la necesidad de recabar el previo consentimiento informado de los titulares de los datos para utilizar los datos personales para otros fines distintos para los que fueron recabados.

V) Que existen determinados datos personales que de acuerdo al art. 9° de la LPDP si están incluidos en listados no necesitan el previo consentimiento del titular (nombres y apellidos, documento de identidad, nacionalidad y fecha de nacimiento).

VI) Que se considera una buena práctica la publicidad de la actuación administrativa del Estado como elemento coadyuvante a la democracia y a la transparencia.

VII) Que la LPDP recoge en el art. 4 literal g) el procedimiento de disociación de los datos que se podría utilizar para no identificar a los titulares.

VIII) Que además en doctrina existe el principio de divisibilidad por el cual cuando un documento posea segmentos públicos y confidenciales se podrán confeccionar versiones públicas de esos documentos.

ATENTO:

A lo establecido en la LPDP y a lo precedentemente expuesto**,** el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

Aconsejar la realización de versiones públicas de los expedientes que se publiquen en su sitio web sin revelar datos personales utilizando la técnica de la disociación y aplicando el principio de divisibilidad.

Firmado por A/P Federico Monteverde
Ing. José Clastornik
Dr. Felipe Rotondo

Dictamen N° 8 de 21 de agosto de 2009.- Se dictamina sobre anteproyecto de decreto de creación del Sistema Integrado de Información del Área Social (SIIAS) en referencia a la Ley N° 18.331

Montevideo, 21 de agosto de 2009

Dictamen Nº 8
Exp. 2009/27
Ref. Adecuación Anteproyecto de Decreto de creación del Sistema Integrado de Información del Área Social (SIIAS), a la Ley N° 18.331

VISTO:

Las implicancias que el Anteproyecto de Decreto del Sistema Integrado de Información del Área Social (SIIAS) puede ocasionar en materia de protección de datos, conforme las disposiciones de la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008.

RESULTANDO:

I) Que por vía de Decreto se pretende la instauración de un Sistema Integrado de Información del Área Social (SIIAS), en el marco de las competencias que por la Ley N° 17.866 se le atribuyen al Ministerio de Desarrollo Social. El SIIAS será el responsable de la gestión del sistema informático que integra información relativa a prestaciones sociales que son otorgadas a los ciudadanos del Uruguay, a través de la gestión de las diversas instituciones del área pública.

II) Que se alude reiteradamente a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) como Organismo impulsor del avance de la sociedad de la información y del Conocimiento y en esa línea del cometido que éste tiene en la promoción del mejor uso de las tecnologías de la información y las comunicaciones en: las personas, las empresas y el Gobierno. Asimismo se destacan los avances generados a nivel nacional en materia de protección de datos personales y su esencial régimen tuitivo; la puesta en práctica de un Certificado de Nacido Vivo de carácter electrónico; y la mayor eficacia y eficiencia en los procesos de diseño, selección y otorgamiento de prestaciones sociales de forma moderna y transparente.

III) Que se prevén como cometidos del SIIAS:

a) Generar un sistema integrado de información interinstitucional que vincule

datos de los distintos organismos, tanto de sus programas sociales, su ejecución y sus respectivos beneficiarios.
b) Contribuir a mejorar la definición de la población objetivo y la implementación de programas sociales a través de la generación, mayor sistematización y disposición de información actualizada.
c) Proporcionar a decisores, gestores, e investigadores una visión integrada de la política social y su alcance, al mismo tiempo que posibilitar la elaboración y el desarrollo de un plan estratégico de políticas sociales de alcance global.
d) Establecer los estándares necesarios para la articulación y coordinación de las diferentes instituciones que realizan políticas sociales integradas al sistema desde la perspectiva de un intercambio sistemático y permanente de información.
e) Modernizar los procesos informáticos de las diferentes dependencias para la entrada, modificación, análisis y evaluación de la información. Impulsar el empleo de la información para la mejor atención a los ciudadanos, propendiendo la puesta en marcha de los procedimientos de corrección de los datos por los responsables de su mantenimiento en cada organismo.
f) Aumentar la eficacia en la gestión de la información de programas sociales, a través de un monitoreo constante de la misma, como base para la mejora de la implementación de dichos programas.
g) Facilitar el acceso de la ciudadanía a la información.

IV) Que se dispone que el Sistema sea de uso público permitiendo para aquellas secciones que así se determine, el acceso a los ciudadanos a la información de prestaciones sociales que brinda el Estado, incorporando los mecanismos de control previstos por la LPDP. Se establece que sea administrado por un Comité de Dirección que estará integrado con un representante de los Organismos involucrados (ASSE, BPS, INAU, MIDES, MSP), el que tendrá diversos cometidos y se preceptúa que todos los Organismos Públicos prestarán colaboración en los aspectos necesarios para el cumplimiento de los cometidos del SIIAS.

V) Que se expidió informe jurídico el 13 de julio de 2009.

CONSIDERANDO:

I) Que si bien en la especie se trata de un intercambio masivo de información, lo que supone la exteriorización de una verdadera "interoperabilidad", ante la ausencia de normativa que hasta el momento regule este aspecto, se debe estar a las disposiciones de la Ley de Protección de Datos Personales y Acción de Habeas Data (LPDP) en materia de comunicación de datos. Esta es definida por el artículo 4 literal B), como *"toda revelación de datos realizada a una persona distinta del titular de los datos"*.
El régimen general de comunicación de datos se encuentra regulado en el artículo 17 que dispone que *"Los datos personales objeto de tratamiento solo podrán ser comunicados para el cumplimiento de fines directamente relaciona-*

dos con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo".
A tal previsión se le adicionan las excepciones establecidas en el artículo 9° de la LPDP. El literal C) exceptúa del previo consentimiento al titular cuando 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 y en el caso de personas jurídicas a razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.
El literal B), por su parte, prevé la hipótesis de que los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. Esta última previsión (existencia de ley) tiene su fuente en la Directiva 95/46/CE, art. 11.2.

II) Que si bien un ideal de regulación del sistema lo sería por vía legal, la introducción del mismo a través de decreto sería viable por cuanto existe una habilitación legal primigenia proveniente de la Ley N° 17.866 y además estaría en juego *"el ejercicio de funciones propias de los poderes del Estado"*, como reclama el literal B) del artículo 9° de la LPDP en remisión del artículo 17 de la misma norma. Esta disposición no establece los dos requerimientos en forma conjunta, sino que es totalmente legítima la comunicación de datos no requiriéndose el previo consentimiento informado del titular, cuando lo sea por una u otra causa, es decir, en virtud del ejercicio de funciones propias de los poderes del Estado o por una obligación legal. La conjunción disyuntiva "o" así lo indica.

III) Que la Ley N° 17.866, de 31 de marzo de 2005 que crea el Ministerio de Desarrollo Social dispone en su artículo 9° literales D y E que a éste le compete: *"Diseñar, organizar y operar un sistema de información social con indicadores relevantes sobre los grupos poblacionales en situaciones de vulnerabilidad, que permita una adecuada focalización del conjunto de políticas y programas sociales nacionales", "Diseñar, organizar y administrar un sistema de identificación, selección y registro único de los núcleos familiares o individuos habilitados para acceder a los programas sociales, sujeto a criterios de objetividad, transparencia, selectividad, temporalidad, y respetando el derecho a la privacidad en los datos que así lo requieran"*. Parece vislumbrase de las funciones propias del Ministerio de Desarrollo Social, que en el cometido de un diseño global de políticas sociales, el SIIAS pretende ser una herramienta fundamental, habida cuenta del objetivo de generar un registro único de personas donde se establezca quiénes son beneficiarios de los programas sociales que brinda el Estado y cuáles son los beneficios que reciben.

IV) Que entre los Organismos involucrados existe un flujo bidireccional, en tanto aportan y consultan información. Entre estos Organismos que integran el

Sistema y aquellos a los que se les solicita cooperación, el flujo de información debe ser sin trabas a los efectos de poder garantizar una mayor eficacia y eficiencia en los procesos de diseño, selección y otorgamiento de prestaciones sociales de forma moderna y transparente. No obstante deberán tener siempre presente los principios de finalidad, veracidad, seguridad y reserva consagrados en la LPDP. Así, los datos que se recojan deberán ser adecuados, ecuánimes y no excesivos en relación con la finalidad; no podrán ser utilizados para finalidades distintas o incompatibles con las que motivaron su recolección; deberán adoptarse medidas de seguridad y confidencialidad; y las personas que se dediquen a la obtención y tratamiento de los datos personales; y guardar estricto secreto profesional, so pena de incurrir en el delito consagrado en el artículo 302 del Código Penal.

V) Que se deberá tenerse particular atención con los datos especialmente protegidos, esto es, los datos sensibles y los relativos a la salud. De acuerdo a la definición que da el artículo 4° de la LPDP, dato sensible es aquel que revela origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual. El artículo 18 edicta que éstos solo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular o cuando medien razones de interés general autorizadas por Ley, cuando el Organismo solicitante tenga mandato legal para hacerlo, o cuando se traten con fines estadísticos o científicos, cuando se disocien de sus titulares. El artículo 19 de la LPDP, por su parte, prevé el tratamiento de los datos relativos a la salud por parte de los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud de los pacientes que acudan a los mismos o que hubieren estado bajo tratamiento de aquellos, respetándose el debido secreto profesional. De manera que en el ejercicio de la actividad de los Organismos involucrados, será estrictamente necesario en la recolección, tratamiento y eventual comunicación de estos datos, el consentimiento expreso del titular.

VI) Que el acceso al público en general deberá ser restringido a los datos que contempla el literal C) del artículo 9° de la LPDP o a aquellos que arrojen datos estadísticos, disociados de sus titulares.

ATENTO:

A lo expuesto y lo dispuesto por las disposiciones legales citadas, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido que el Anteproyecto de Decreto no vulnerara disposiciones de la Ley Nº 18.331, con las precisiones referidas en los considerandos.

2) Recomendar que el artículo 2° del Anteproyecto de Decreto quede redactado de la siguiente manera:

"Este Sistema permitirá el libre flujo de información entre los Organismos Públicos involucrados y aquellos de igual naturaleza que se les solicite colaboración en el marco del cumplimiento de los cometidos del SIIAS, respetándose especialmente los principios de finalidad, veracidad, reserva y seguridad consagrados en la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008.

En la recolección, tratamiento y comunicación de datos sensibles entre los Organismos involucrados, será necesario el previo consentimiento expreso del titular de los datos.

Fuera de los casos contemplados en el inciso anterior, el acceso público será limitado a los datos estadísticos o a aquellos que sin revestir ese carácter se encuentren disociados de sus titulares".

Firmado por A/P Federico Monteverde

Dictamen N° 9 de 28 de agosto de 2009.- Se dictamina sobre una consulta remitida por la Unidad de Acceso a la Información Pública, referida al carácter público o confidencial de determinada documentación provista por terceros, que se encuentra en poder de la Intendencia Municipal de Montevideo

Montevideo, 28 de agosto de 2009

Dictamen Nº 9
Exp. Nº 2009/030
Ref. Solicitud de información relativa al carácter público de determinada documentación en poder de la I.M.M. y las vías correctas para su obtención.

VISTO:

La consulta formulada por el Sr. Marcelo Caffera ante la Unidad de Acceso a la Información Pública, acerca de si la información que detalla es pública y si es factible que pueda obtenerla, amparado en la Ley N° 18.381 de Acceso a la Información Pública, de 17 de octubre de 2008 .

RESULTANDO:

I) Que el objeto de la consulta refiere a los datos que las plantas industriales sitas en Montevideo deben entregar cuatrimestralmente a la Unidad de Efluentes Industriales de la Intendencia Municipal de Montevideo.

II) Que se expide informe jurídico (fs. 24-25), solicitando en carácter de complementariedad, se eleve el expediente en consulta a la Unidad Reguladora y de Control de Datos Personales (URCDP) para que se pronuncie desde el punto de vista de la protección de datos personales acerca de: *"a) si los reseñados datos pueden entenderse incluidos en la referencia efectuada; b) si la disociación de la información es un elemento factible a ser informado al consultante a los efectos de obtener al menos esta información de parte de la requerida"* (fs. 26-27).

III) Remitido el expediente a la URCDP, se emite informe (fs. 29-30), elevándose al Consejo Ejecutivo de la Unidad, el 10 de agosto de 2009 (fs. 30 vto.).

CONSIDERANDO:

I) Que el punto objeto de consulta refiere concretamente a la información sobre el número de empleados que trabajan en cada turno en forma mensual y el total de productos confeccionados al mes por las empresas.

II) Que no toda información personal en poder de un Organismo Público puede

ser cedida por el solo hecho de estar incorporada en un registro público. El artículo 8° de la Ley N° 18.381 prevé entre las excepciones a la información pública, las definidas como secretas por la Ley y las que se definan como reservada o confidencial, (artículos 9° y 10). El artículo 10 establece que se considera información confidencial, entre otras, aquella que *"refiera al patrimonio de la persona; comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica que pudiera ser útil para un competidor* (literales A) y B) del numeral I); y *"Los datos personales que requieran previo consentimiento informado"* (numeral II).

III) Que una vez analizadas las disposiciones que regulan el derecho de acceso y sus excepciones, resulta oportuno aludir a las disposiciones de la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data (en adelante LPDP), de 11 de agosto de 2008.

La transmisión de información a que refiere la consulta supone una comunicación de datos de carácter personal, definida por el artículo 4° literal B) de la LPDP como *"toda revelación de datos realizada a una persona distinta del titular de los datos"*. El artículo 17 de la LPDP que regula los derechos referentes a la comunicación de datos, establece que *"Los datos personales objeto de tratamiento solo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo"*. Es decir que se requieren ambos requisitos conjuntamente: el interés legítimo del emisor y del destinatario y el previo consentimiento del titular de los datos, respetándose el principio de finalidad, de manera que los datos que fueron recabados para un fin no sean destinados para otro.

El artículo 17 dispone que el previo consentimiento no será necesario cuando: lo disponga una ley de interés general; en los supuestos del artículo 9° de la Ley; 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; se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

A su vez, el artículo 9° prevé que no será necesario el previo consentimiento cuando: los datos provengan de fuentes públicas de información; se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; 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.

IV) Que la información que se solicita en tanto refiere al número de empleados que trabajan en cada turno en forma mensual y al total de productos confeccionados al mes por las empresas, no resulta abarcada por las excepciones que contempla el artículo 9° al que se remite el artículo 17 de la LPDP. En consecuencia, esta información, puede ser comunicada con el previo consentimiento informado del titular de los datos y mediante la acreditación de un interés legítimo, esto es, un interés personal y directo que demuestre la necesidad de acceder a dicha información, respetándose los principios consagrados en la LPDP, esencialmente los de finalidad, seguridad y reserva (artículos 8°, 10 y 11).

No obstante, podrá brindarse la información que se solicita sin sujetarse a los requerimientos antedichos, siempre que se aplique un procedimiento de disociación, de manera que los titulares de los datos no puedan ser determinables. Adviértase que las disposiciones de la LPDP resultan aplicables a los datos personales, es decir a aquella *"información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables"*. (artículo 4°, literal D)

ATENTO:

A lo expuesto y a lo previsto por las disposiciones legales citadas, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido plasmado en el numeral IV) de los Considerandos.

2) Notifíquese, publíquese y oportunamente archívese.

Firmado por A/P Federico Monteverde

Dictamen N° 14 de 25 de setiembre de 2009.- Se dictamina sobre una consulta remitida por la Unidad de Acceso a la Información Pública, sobre las posibilidades de obtener por la Facultad de Ciencias Económicas el padrón de egresados con sus correspondientes direcciones electrónicas

Montevideo, 25 de setiembre de 2009

Dictamen Nº 14
Exp. Nº 2009/005 UAIP
Consulta relativa a las posibilidades de obtener de parte de la Facultad de Ciencias Económicas el padrón de egresados con sus correspondientes direcciones electrónicas o incluso éstas disociadas, al amparo de la Ley Nº 18.381.

VISTO:

Estos obrados remitidos por la Unidad de Acceso a la Información Pública.

RESULTANDO:

I) Que este Consejo se limitará a resolver, con carácter de dictamen, si la aspiración de un Consejero de una Facultad perteneciente a la Universidad de la República en cuanto a solicitar y obtener los correos electrónicos de los egresados de dicha Facultad, encuadra dentro de la Ley Nº 18.331 de Protección de Datos Personales y Acción de "Habeas Data" de 11-08-2009.

II) Que con fecha 15 de setiembre de 2009 se emitió el Informe jurídico correspondiente.

CONSIDERANDO:

I) Que la respuesta a esta aspiración será negativa, en orden a los argumentos y fundamentos que pasan a exponerse.

II) Que ante todo debe apreciarse que el integrante de un órgano colegiado regido por el Derecho Público, como es el caso, carece de legitimación para pretender este tipo de informaciones a título individual, ya que todos sus actos deben revestir un carácter oficial para considerarlos legítimos, que permita identificarlos clara e inequívocamente como actividades preparatorias enderezadas a formar la voluntad del órgano al que pertenece el miembro en cuestión.

III) Que así lo tiene consignado la *opinio doctrinalis* en aplicación de la Teoría del Órgano desarrollada en el Derecho Administrativo, donde se distingue claramente "cargo", "órgano" y "persona jurídica": *"Las situaciones jurídicas abstractamente atri-*

buidas a un cargo pueden implicar una actividad material o intelectual de quien lo ocupa; toda ella se atribuye como actividad de la persona jurídica. Cuando el derecho dispone que cierta actividad intelectual del titular del cargo se atribuya a la persona jurídica como un `acto jurídico´, determinación de la voluntad* jurídica *de la persona jurídica, el cargo en cuestión forma parte de un `órgano´ de esa persona. Sólo ese contenido de la actividad atribuida por una norma jurídica hace que el cargo se considere formando parte de un órgano, porque esa es la razón de ser del concepto mismo de órgano: explicar que la actividad intelectual de una persona física se atribuya a un sujeto de derecho distinto, la persona jurídica, como determinación de su voluntad jurídica". (CAJARVILLE PELUFFO, Juan Pablo - "Sobre Derecho Administrativo" Tomo I, 2ª edición ampliada, FCU, 2008, p. 498).

IV) Que en cuanto al llamado "procedimiento colegial", que culmina finalmente con el acto administrativo propiamente dicho, se agrega de modo concordante: *"Cuando el órgano es compuesto, aquella sucesión ordenada de acontecimientos del mundo exterior ubicados en el espacio y en el tiempo, que consisten generalmente en comportamientos voluntarios del o los titulares del órgano, a los cuales el derecho confiere la relevancia de perfeccionar la voluntad del órgano, constituyen un procedimiento interno, el llamado `procedimiento colegial´, en el que cabe distinguir varias etapas: convocatoria, instalación, deliberación, votación y formulación del acto propiamente dicha."* (CAJARVILLE PELUFFO, op. cit. p. 506).V

V) Que la Ley Nº 12.549 de 29-10-1958 (Ley Orgánica de la UDELAR) rige la especie y la misma no contiene norma alguna que habilite a un Consejero de Facultad, a título particular o individual, a llevar a cabo este tipo de requerimientos, en tanto el cuerpo legal alude a "atribuciones" solamente de los Consejos de las Facultades, los Decanos y las Asambleas del Claustro (Cap. VI, arts. 39 y sigtes), pero en ningún caso de los Consejeros actuando de la manera que pretende el promotor de autos, y ni siquiera sumando voluntades dispersas de otros Consejeros a la suya propia.

VI) Que el pretendido acto, si se llevara a cabo en los hechos, violentaría también el sistema jurídico de competencia específica de esta Unidad Reguladora y de Control, comenzando por destacarse que el correo electrónico contiene o es en sí mismo un dato personal, puesto que contiene "información... referida a personas físicas o jurídicas, determinadas o determinables" (art. 4 de la Ley Nº 18.331 de 11-08-2008).

VII) Que enfocando situaciones similares ocurridas en España se ha podido afirmar lo siguiente: *"Con carácter general, los datos personales del estudiante únicamente podrán ser recogidos, tratados y cedidos, incluso sin el consentimiento del afectado, para el desarrollo y mantenimiento de la relación administrativa existente entre el alumno y la Universidad (vg. Carnet oficial de estudiante), y dentro del marco de las funciones administrativas atribuidas por la normativa aplicable a la propia Universidad."* (AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID - "Protección de datos personales para Universidades", Ed. Thomson-Civitas, Madrid, 2008, p.148).

VIII) Que la situación sub-examine encuadra, pero en forma negativa, en la figura legal de "comunicación de datos personales" (art. 17 de la Ley Nº 18.331), a cuyo respecto surge sin lugar a dudas la necesidad de cumplir una serie de previsiones que están también consignadas en la Ley de la materia, y que este hipotética solicitud no cumpliría, a saber:

• actuación de los responsables ajustada a los principios de la base de datos, y en general de todos quienes actúen en relación a datos personales (art. 5 acápite de la Ley);
• principio de finalidad, en cuanto a que los datos objeto de tratamiento no sean utilizados para propósitos distintos o incompatibles con los que motivaron su demanda y obtención originarias (art. 8 de la Ley);
• principio de previo consentimiento informado de los titulares de estos correos electrónicos al suministrarlos a la Facultad (art. 9 de la Ley), a lo que se suma la no figuración de este tipo de datos entre las hipótesis de excepción que no requieren tal consentimiento (arts. 9 tercer inciso y 17 de la Ley);
• el propio régimen legal de la comunicación de datos que, además de lo relativo al consentimiento del titular (remisión al item inmediato anterior) contiene también otros deberes y previsiones que no se compadecen con la pretendida solicitud: interés legítimo del emisor y del destinatario (remisión a Considerandos II a V de este Dictamen); cumplimiento de fines relacionados a esos intereses, no a otros (remisión al principio de finalidad).
• imposibilidad de aplicar en el caso procedimientos de disociación para suministrar información exenta de datos personales (art. 17 último inciso, de la Ley).

IX) Que de acuerdo con los arts. 2, 8 y 10 numeral II de la Ley N° 18.381, se entiende que los datos personales cuyo registro y tratamiento por organismos públicos (estatales y no estatales) requiere consentimiento de sus titulares, son información confidencial y, como tal, están excluidos del derecho de acceso a la información pública.

ATENTO:

A lo expuesto y lo dispuesto por el artículo 21 literal D de la Ley Nº 18.331, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

Declarar que la solicitud de correos electrónicos de estudiantes o egresados de las Facultades pertenecientes a la Universidad de la República, por parte de un Consejero de la misma, no es conforme a derecho.

Firmado por A/P Federico Monteverde

Dictamen N° 16 de 23 de octubre de 2009.- Se dictamina sobre consulta referida a evaluar el carácter de fuentes públicas de las guías telefónicas

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Montevideo,23 de octubre de 2009

VISTO:

La consulta formulada a efectos de analizar el carácter de fuente pública de las guías telefónicas emitidas con anterioridad y posterioridad a la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP).

RESULTANDO:

I) Que la LPDP consagró el derecho fundamental a la protección de datos personales y estableció que su régimen será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento.

II) Que resulta pertinente determinar el régimen legal de las guías telefónicas emitidas antes de la entrada en vigencia de la LPDP y de las que se emitieren en el futuro.

CONSIDERANDO:

I) Que existen diversas soluciones sobre el punto en el derecho comparado, recogiéndose en algunos casos el requisito del previo consentimiento informado para la inclusión en un repertorio telefónico; o considerándolo como una fuente accesible al público, sin que sea necesario cumplir con aquel requisito.

II) Que la LPDP y su decreto reglamentario N° 414/009 establecen que en el caso de las personas físicas, el teléfono es un dato personal que requiere el previo consentimiento informado del titular del servicio, no así en el caso de las personas jurídicas, que está incluido expresamente dentro de las excepciones del artículo 9°, literal C) de la LPDP.

III) Que hasta la sanción de la LPDP consuetudinariamente las guías telefónicas fueron consideradas fuentes públicas de información en tanto estaban a dis-

posición de cualquier persona que deseara consultarlas, en cualquier propiedad privada, entidad pública o empresa, de cualquier punto del país.

IV) Que si bien el artículo 46 de la LPDP establece que las Bases de Datos deberán adecuarse a sus disposiciones dentro del plazo de un año de la entrada en vigor, las guías telefónicas -bases de datos de acuerdo a la definición que brinda el artículo 4°, literal A)- por su especial naturaleza, merecen un tratamiento disímil.

V) Que tomando en consideración las soluciones del derecho comparado y aplicando el principio de realidad, corresponde considerar a las guías telefónicas emitidas hasta el 11 de agosto de 2008 (fecha de sanción de la LPDP), como fuentes públicas de información.

VI) Que a partir de la entrada en vigencia de la LPDP, para la emisión de nuevas guías telefónicas se deberá recolectar el consentimiento de los nuevos titulares del servicio telefónico, de forma previa, conforme lo previsto en el artículo 9° de la LPDP, cumpliendo con los requisitos allí contemplados.

VII) Que si bien se tiene conocimiento que en la actualidad la exclusión de guía ya no reviste el carácter de onerosa, deberá tenerse especial atención en la gratuidad del derecho de no inclusión.

ATENTO:

A lo expuesto y a lo previsto por las disposiciones legales citadas, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido plasmado en los numerales V a VII de los Considerandos.

2) Notifíquese y oportunamente, publíquese.

Firmado por A/P Federico Monteverde

Dictamen N° 18 de 9 de diciembre de 2009.- Se amplía Dictamen N° 16 de 23 de octubre de 2009

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Montevideo, 9 de diciembre de 2009

VISTO:

La consulta formulada a efectos de analizar el carácter de fuente pública de las guías telefónicas emitidas con anterioridad y posterioridad a la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP), la contemplación de su regulación on line y su posible vinculación con la reciente Ley N° 18.600, de 21 de septiembre de 2009.

RESULTANDO:

I) Que se emitió informe N° 104 de 3 de noviembre de 2009, ampliando informe N° 92 de 29 de octubre de 2009.

CONSIDERANDO:

I) Que en el Dictamen N° 16 de 23 de octubre de 2009 se estableció que las guías telefónicas que fueron emitidas con anterioridad a la sanción de la LPDP deben ser consideradas fuentes públicas de información. Ahora bien, corresponde delimitar el alcance de la normativa, en el sentido que lo dispuesto en el considerando V) del dictamen aludido, es sin perjuicio de lo que prevé el artículo 46 de la LPDP respecto al período de un año de adecuación.

II) Que la Ley N° 18.600 viene a confirmar que la guía telefónica se categoriza como documento electrónico, teniendo la misma validez y eficacia probatoria que el documento tradicional, por lo que el soporte en el que se encuentre contenido es indiferente.

III) Que las guías telefónicas, tanto convencionales como informatizadas emitidas hasta el 11 de agosto de 2009 -plazo en el que venció el año de adecuación se pueden considerar fuentes públicas de información, no así las que se emitan con posterioridad a esa fecha, donde se deberá recabar el previo consentimiento de los titulares de los servicios telefónicos, de acuerdo con lo preceptuado por el artículo 9° de la LPDP.

ATENTO:

A lo expuesto, al informe incorporado a fs. 7 y a lo previsto por las disposiciones legales citadas, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido establecido en los numerales I a III de los Considerandos.

2) Notifíquese y oportunamente, publíquese.

Firmado por A/P Federico Monteverde
m.j.r.

Dictamen N° 19 de 17 de diciembre de 2009.- Se dictamina sobre una consulta referida al alcance de los artículos 28 y 29 de la Ley N° 18.331

Montevideo, 17 de diciembre de 2009

Dictamen Nº 19
Exp. Nº 063/2009
Ref. Consulta técnica sobre alcance de los arts. 28 y 29 de la Ley Nº 18.331

VISTO:

La consulta formulada sobre el alcance de los artículos 28 y 29 de la Ley Nº 18.331 de 11 de agosto de 2008.

RESULTANDO:

I) Que el consultante entiende que las personas físicas y jurídicas, constituyan empresas o no, no quedan obligadas al registro de datos consignados en bases de datos o fuera de ellas, cuando se trata de uso exclusivamente interno o personal.

II) Que en defensa de su postura sostiene que la referencia a "uso exclusivamente individual o doméstico" del art. 28 no puede aludir sino a las personas jurídicas, puesto que el mismo tipo de referencia está contenida en el art. 3 lit. C para personas físicas, y como principio una norma jurídica debe interpretarse sin redundancias.

III) Que agrega otros razonamientos, que a su juicio, conducen a la misma conclusión, a saber: que el titular de una persona jurídica es en definitiva una persona física, y como tal no deben existir distingos de régimen o requisitos, de una categoría a otra; que conforme doctrina que cita, el legislador previó como circunstancias que excluyen el registro de la base de datos, que se trate de uso personal del propio sujeto y su familia -en el caso de persona física-, o bien se trate de uso exclusivo interno de la sociedad -en el caso de la persona jurídica-. (DURÁN MARTÍNEZ, Augusto, "Derecho a la Protección de Datos Personales y al Acceso a la Información Pública Leyes 18.331 y 18.381 AMF 2009 pág. 86).

IV) Que asimismo entiende que la precisión contenida en el art. 15 lit. B, segundo párrafo del Decreto Nº 414/009 de 31 de agosto de 2009 debe desaplicarse por exceder el ámbito reglamentario (no aplicación de la excepción de ámbi-

to personal o doméstico vía art. 3 lit. A de la ley a las personas jurídicas).

CONSIDERANDO:

I) Que las fuentes europeas en que se funda nuestro régimen jurídico en la materia, enseñan lo contrario a la tesis aportada por el consultante y las fuentes que emplea en su apoyo, estableciendo con toda claridad que solamente las personas físicas pueden poseer un ámbito personal o doméstico (cf. Directiva de la UE 95/46/CE, art. 3.2 segundo guión y Considerando 12; Dictamen 4/2004 del Grupo de Trabajo del Art. 29; Sentencia del 6 de noviembre de 2003 del TSJ de la CEE, caso Lindqvist).

II) Que lo propio cabe concluir en el derecho español, donde son varias las normas que vinculan el ámbito personal o doméstico exclusivamente a la persona física, y más precisamente a los "particulares", expresión que deja fuera del excepcionamiento a los profesionales (art. 2.2a de la LOPD, art. 4 primer párrafo del Reglamento, art. 1.3 de la Instrucción 1/2006 de 8 de noviembre sobre tratamiento de datos personales con fines de videovigilancia).

III) Que por definición, una persona jurídica carece de "ámbito personal o doméstico", atento a que el reconocimiento y las manifestaciones de la "personalidad jurídica", en el caso de las personas morales, resulta absolutamente incompatible con la ausencia de control estatal externo que supone aquél ámbito, estando una persona moral, cualquiera sea ella, sometida en todo momento a los poderes de control del Estado, cosa que no sucede con la persona física.

IV) Que la diferenciación anotada en el numeral anterior, encuentra perfecta coherencia con el art. 2 de la Ley Nº 18.331 de 11 de agosto de 2008, de donde surge que el dispositivo proteccionista (que entre otros elementos abarca ser excluido o excepcionado del ámbito objetivo de la ley en función de preservar un ámbito intimista) se extiende a las personas jurídicas, pero tan solo "en cuanto corresponda", quedando fuera de tal consideración -por tanto- el ámbito personal o doméstico.

V) Que es dable tener presente en todo momento, que el principio proteccionista articulado a partir de la Ley Nº 18.331, constituye elemento de inspiración básico para interpretar correctamente esta regla de derecho positivo, que tiene como uno de sus pilares el registro de las bases de datos personales, siendo las excepciones al régimen, de interpretación estricta, como cualquier excepción a una regla jurídica, máxime en sede de derechos fundamentales inherentes a la personalidad humana (art. 72 de la Constitución de la República, art. 1º de la Ley Nº 18.331).

VI) Que se emitió en autos informe jurídico extensivo en el sentido apuntado en el presente dictamen, y se tendrá presente que la Unidad ya se ha pronuncia-

do con anterioridad sobre el mismo tópico en consulta.

ATENTO:

A lo expuesto, a lo dispuesto por el artículo 34 literal A de la Ley Nº 18.331 de 11 de agosto de 2008, y lo consignado en el Dictamen Nº 10 de 11 de setiembre de 2009, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

Que el art. 15 lit. B segundo párrafo del Decreto Nº 414/009 de 31 de agosto de 2001 es legal, al ilustrar lo que está dispuesto por disposiciones constitucionales y legales en cuanto a que las personas jurídicas o morales carecen en todos los casos de "ámbito personal, individual o doméstico".

Firmado por A/P Federico Monteverde

Dictamen N° 20 de 30 de diciembre de 2009.- Se dictamina sobre consulta referida a si los números de cédula de identidad incorporados al expediente electrónico violentan la Ley N° 18.331

Montevideo, 30 de diciembre de 2009

Dictamen Nº 20
Exp. 2009/244
Ref. Consulta sobre números de cédula identidad incorporados a expediente electrónico

VISTO:

El planteo realizado sobre números de cédula de identidad incorporados a expediente electrónico.

RESULTANDO:

I) Que el solicitante cuestiona si el número de cédula de identidad (sin puntos ni guiones) definido como usuario del sistema en el proyecto de expediente electrónico para el MIEM, violenta la Ley N° 18.331.

II) Que se expidió el informe jurídico N° 270, el 21 de diciembre de 2009.

CONSIDERANDO:

I) Que el artículo 4° de la LPDP define dato personal como *"información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables",* incluyéndose por ende la cédula de identidad como dato personal.

II) Que el artículo 9° de la LPDP que regula el principio del previo consentimiento informado, dispone que el tratamiento de datos personales será lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, no siendo necesario 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.

III) Que la excepción del literal c) incluye al documento de identidad, a texto expreso, como dato exento del previo consentimiento para su tratamiento.

IV) Que la excepción del literal b) también resultaría abarcada en el presente, por cuanto el expediente electrónico propone garantizar una mayor transparencia en el manejo de la información, a la vez que promete una mayor eficiencia en la tramitación en la Administración Pública, con el consecuente beneficio que esto reporta, no solo en cuanto a la gestión en si misma, sino a la celeridad en que se desarrollarán los trámites.

ATENTO:

A lo expuesto y lo dispuesto por las disposiciones legales citadas, la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido que el número de cédula de identidad definido como usuario del sistema en el proyecto de expediente electrónico para el MIEM no violenta la normativa de protección de datos personales (Ley N° 18.331 y decreto reglamentario N° 414/009 de 31 de agosto de 2009).

2) Notifíquese, publíquese y oportunamente archívese.

Firmado por A/P Federico Monteverde
m.j.r.

Informe N° 7 de 15 de abril de 2009.- Se informa sobre la procedencia de la publicación en el sitio web del Ministerio de Salud Pública de las otras actividades declaradas por los inspectores del mencionado Ministerio

Montevideo, 15 de abril de 2009

Informe N° 7
Exp. 008/009
Ref.: Publicación en web de otras actividades laborales declaradas por inspectores del M.S.P.

Antecedentes

Con fecha 12 de marzo de 2009 el Dr. Jorge Basso Garrido, en representación del Ministerio de Salud Pública, solicita opinión a la Secretaría de Presidencia de la República concerniente a la posibilidad de publicar en la página web información acerca de las demás actividades laborales declaradas por los inspectores del MSP, sin lesionar disposiciones legales y a efectos de dar mayor transparencia a la gestión.
El expediente pasó en consulta a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) el 16 de marzo de 2009, el que fue recibido por ésta el 18 de marzo de 2009. Con fecha 24 de marzo de 2009 AGESIC remitió el expediente a la Unidad Reguladora y de Control de Datos Personales (URCDP).

Análisis

La situación planteada refiere a aspectos relacionados con la necesidad o no del previo consentimiento para su publicación. En otras palabras, si es necesaria la existencia del previo consentimiento informado o si se puede exceptuar del mismo por entender que se recaban para el ejercicio de las funciones propias de los poderes del Estado. Por tanto, cabe analizar si la publicación en web de otras actividades laborales declaradas por los Inspectores del M.S.P. queda incluida dentro de las funciones propias de éste.
Según Sayagués los organismos tienen determinados cometidos entendiendo por tales: "(…) *las diversas actividades o tareas que tienen a su cargo las entidades estatales conforme al derecho vigente. Su extensión es muy variable y depende de las ideas predominantes acerca de los fines del Estado*. (…)". (Sayagués, FCU, Tomo I, pág. 66).
Si bien el consultante no hace mención respecto a la incompatibilidad del funcionario inspector para desarrollar otras actividades fuera del ámbito del Ministerio, sólo de existir tal incompatibilidad podría estar dada la excepción conteni-

da en el literal B) del art. 9° de la Ley Nº 18.331, de 11 de agosto de 2008. Es decir, tomando en consideración la amplitud de los cometidos que puede tener esa Secretaría de Estado y que en la situación de marras lo que se busca es lograr la mayor transparencia en la gestión, podría entenderse que en el caso concreto es aplicable dicha excepción.

Por otro lado la situación planteada conforma una comunicación de datos de acuerdo a lo previsto en el art. 17 de la Ley N° 18.331. Esta establece que los datos personales "*sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le deberá informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo*".

Es necesario analizar la existencia del interés legítimo. En cuanto al interés del Ministerio, de la breve información proporcionada, se podría inferir que sería necesario a efectos de lograr la mayor transparencia en la gestión del Ministerio.

Con respecto a la excepción contenida en el literal C) se entiende que "*las demás actividades laborales*" constituyen datos personales por lo que se requiere el previo consentimiento ya que la enumeración realizada es taxativa y no comprende dichos datos.

El literal D) que establece que no será necesario el previo consentimiento si se deriva de "*una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento*", en el caso se verificaría esta excepción si se dieran las condiciones expresadas al analizar el literal B), es decir, si se considera que para poder ejercer la tarea es necesario informar de la existencia de otra actividad.

Conclusiones

De acuerdo a lo anteriormente expuesto y tomando en cuenta la sucinta información brindada corresponde informar que se podrán publicar las demás actividades laborales de los Inspectores del MSP si se entiende que forma parte de las funciones propias del organismo y teniendo en consideración el logro de la mayor transparencia de la gestión. En consecuencia y de darse la existencia de la hipótesis mencionada, no sería necesario el previo consentimiento porque se exoneraría de acuerdo a lo dispuesto en el literal B) del art. 9° de la Ley Nº 18.331. En caso contrario se deberá recabar el previo consentimiento informado de acuerdo a las previsiones contenidas en dicho artículo.

Dra. Flavia A. Baladán
Derechos Ciudadanos

Informe N° 12 de 28 de abril de 2009.- Se informa sobre la adecuación del Anteproyecto de Ley Catastral a la Ley N° 18.331

Montevideo, 28 de Abril de 2009

Informe Nº 12
Exp. 2009/11
Ref. Consulta sobre Anteproyecto de ley catastral

La presente consulta viene a consideración de esta Unidad, conforme lo previsto en el art. 34 literal f) de la Ley de Protección de Datos Personales Nº 18.331 (en adelante LPDP), ante requerimiento de la Dirección Nacional de Catastro solicitando evaluación del Anteproyecto de Ley Catastral que adjunta, con relación a la materia competencia de esta Unidad.

Analizado el Anteproyecto de referencia no se observan confluencias notables con el régimen jurídico vigente en sede de protección de datos personales, a reserva de tres puntos o aspectos, uno de ellos de índole genérica (punto 1) y los restantes más específicos (puntos 2 y 3). Estas posibles zonas de confluencia son las siguientes:

1) Contenido que pudieran asumir los registros e informaciones recogidos, tratados y eventualmente suministrados nuevamente a terceros por la DNC, de acuerdo al nuevo régimen proyectado (arts. 4 literales d, e, g, h, k,i; 8, 11, 12, 13, 16).

2) Cometido de "llevar y administrar el registro de los Profesionales habilitados para presentar documentación catastral ante la DNC" (art. 4 literal m del Anteproyecto de Ley).

3) Cometido de "aplicar sanciones a los Profesionales habilitados para presentar documentación catastral ante la Dirección Nacional de Catastro" (art. 4 literal n del Anteproyecto de Ley).

Con respecto al primer punto, se advierte que el Anteproyecto de Ley menciona en varios tramos de su articulado algunos actos y actividades que podrían llegar a referir o involucrar datos personales, si bien el proyectado texto legal nada sugiere explícitamente al respecto .

Se trata de textos generales y abiertos, por lo que, de no fijarse en la reglamentación posterior un criterio que evite lo más posible la utilización de datos personales, o al menos se maneje con criterios restrictivos y finalistas, se podría llegar a incumplir los

principios consagrados en los arts. 7 y 8 de la Ley 18.331, en cuanto a utilización de datos "no excesivos" y "compatibles con la finalidad de su obtención".

No escapa al entendimiento del informante que la hipótesis de conflicto de las citadas normas con el régimen jurídico de protección de datos personales en este nivel del análisis, podría darse recién en la etapa posterior reglamentaria, y de un modo posiblemente indirecto, en virtud de la propia naturaleza del "dato catastral", de principio diferente y ajeno al "dato personal". De todas formas se advierte, siguiendo el hilo argumental, el eventual conflicto que podría tener lugar desde el momento que" dato personal" no es solamente aquel dato que identifica a las personas, sino también aquella información que las hace "identificables" (art. 4 literal d de la Ley 18.331). Por lo que perfectamente puede llegar a concebirse (al menos como una posibilidad y si no se pusiese el cuidado sugerido en la reglamentación), que alguno de los citados actos o actividades permitiesen derivar la identificación de personas físicas o jurídicas propietarias de inmuebles a partir de "datos catastrales típicos", como ser números de padrón, identificación de calle y número de puerta.

Por este tipo de consideraciones, y en tanto la actividad acometida y costos involucrados lo permitan, es que se aconseja "disociar" la información en los términos estatuidos por los arts. 4 literal G y 17 inc. 3 literal D de la Ley 18.331, ante cualquier sospecha de interferencia o exigencia insalvable del régimen proyectado, con el actualmente vigente en materia de datos personales. Aún cuando –se reitera- no cabe inferir de la letra del Anteproyecto de Ley en examen, pero sí eventualmente de una reglamentación posterior que no pusiera cuidado a estos aspectos, que tal interferencia o colisión llegue a ocurrir.

Con respecto al segundo punto del presente informe, no cabe duda que el art. 4 literal m del Anteproyecto de Ley alude, y aquí sí de modo directo, a una actividad que ingresa sin ambajes o escalonamientos normativos dentro del ámbito de la Ley 18.331.

La operación de "llevar y administrar el registro de los Profesionales habilitados…" debe adecuarse a los preceptos de la Ley 18.331. En este punto consideramos que no cabrá excluir esta actividad del ámbito de aplicación de la ley 18.331 por vía del art. 3 inc. 2 literal C de esta última, inaplicable a la especie. La precitada norma excluyente merece interpretación estricta en su lectura ("…bases de datos creadas y reguladas por leyes especiales) por lo que, a juicio del informante, al no surgir del Anteproyecto una sustantiva "regulación" de tales bases sino su mera previsión, y al no tratarse de "ley especial" conforme exige la norma excluyente, se deberá entender que este registro resulta regulado por la Ley 18.331 en total plenitud.

Finalmente el tercer punto del presente informe enfoca al art. 4 literal n del Anteproyecto de Ley en relación régimen de protección de datos. Los actos previstos en el proyectado artículo-literal (aplicación de sanciones a profesionales universitarios) remiten de modo expreso, en este caso, a una reglamentación posterior, la que, a igual título y consideración que el punto 2,

deberá atenerse en un todo a las previsiones de la Ley 18.331.

Conclusiones

1) El Anteproyecto de Ley en examen se adecua como tal al régimen jurídico vigente en materia de protección de datos personales, que emana fundamentalmente de la Ley 18.331.

2) Algunas normas de su articulado contienen previsiones que, en etapa de reglamentación posterior, deberían dictarse conforme el régimen precitado para evitar futuras colisiones, directas o indirectas, con el régimen de competencia de la Unidad (arts. 4 literales d, e, g, h, k,i; 8, 11, 12, 13, 16).

3) El art. 4 literal m del Anteproyecto refiere a una actividad típicamente enmarcada dentro de la Ley 18.331, y no excluida de ella atento a la no aplicación del art. 3 inc. 2 literal C de esta última. Como tal, este registro debería crearse y llevarse a cabo en su momento a plena conformidad del régimen en la materia, entre otros aspectos debiendo inscribirse la base de datos ante la Unidad Reguladora y de Control con los requisitos del art. 29 de la Ley 18.331 y su inminente reglamentación.

4) El art. 4 literal n del Anteproyecto, si bien no refiere a bases de datos o registros como el literal anterior del mismo artículo, de todas maneras involucra datos personales y remite de modo expreso, en este punto, a casos y formalidades a establecerse por la reglamentación. Por lo que en la etapa oportuna habría que tener presente la misma advertencia enunciada en numeral supra 2.

5) En tanto y cuanto se creen bases de datos como la prevista en el art. 4 literal m del Anteproyecto (y eventualmente la que pudiera devenir a partir de la desenvoltura reglamentaria del art. 4 literal n), o cualesquiera otras, todas ellas deberían cumplir los principios, derechos de titulares, protección especial para datos sensibles e inscripción de las bases de datos así creadas, al tenor del régimen consgrado por la Ley 18.331.

6) Ante cualquier sospecha de interferencia o exigencia del régimen proyectado, con el actualmente vigente en materia de datos personales, es aconsejable acudir a procedimientos de "disociación de datos" según arts. 4 literal G y 17 inc. 3 literal D de la Ley 18.331.

Firmado por Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 17 de 13 de mayo de 2009.- Se informa sobre el alcance del artículo 12 de la Ley N° 18.381, de Acceso a la Información Pública, desde la perspectiva del régimen jurídico de la protección de datos personales

Montevideo, 13 de Mayo de 2009

Informe Nº 17
Ref. Análisis del artículo 12 de la Ley Nº 18.381 de Acceso a la Información Pública, desde la perspectiva del régimen jurídico de protección de datos personales.

I - Introducción

La norma de inoponibilidad consagrada en el art. 12 de la Ley 18.381 (en adelante Ley de Acceso) nos enfrenta al problema de la armonización de dos o más derechos fundamentales a hacerse valer en simultáneo, en el caso que nos interesa el "derecho de acceso a la información pública" y el "derecho a la protección de los datos personales".
Ante un pedido concreto de información de contenido encuadrado en el art. 12 de la Ley de Acceso (*"... violaciones de derechos humanos o sea relevante para investigar, prevenir, evitar violaciones de los mismos"*), se abren cuatro alternativas:

1) Que el pedido no involucre datos personales, en el sentido preciso que fija la ley de la materia (art. 4 lit. D Ley 18.331, en adelante LPDP).

2) Que el pedido de información refiera a una clase de datos personales, cuyo registro susceptible de tratamientos y usos posteriores quedan fuera del ámbito objetivo de la LPDP, al tenor del art. 3 segundo párrafo de la misma.

3) Que el pedido refiera a una clase de datos de esta naturaleza cuyo recolección y tratamiento no requieran el previo consentimiento informado del titular conforme al artículo 9 LPDP.

4) Que el pedido, finalmente, refiera a datos personales incluidos dentro del ámbito objetivo de la LPDP, y a su vez no excluidos del principio de previo consentimiento informado del titular; en otras palabras: datos personales bajo regulación plena de la LPDP.

En el primer caso, el art. 12 de la Ley de Acceso se aplica sin comentario o problemática de especie alguna, en tanto no estamos en presencia de un dato personal, cuanto menos en el sentido que regula y ampara la ley de la materia. En otras palabras, no valdrá la invocación al amparo de reserva alguna, y, por el contrario deberá darse acceso a la información solicitada.

En el segundo caso, también tendrá aplicación el precitado art. 12 de la Ley de Acceso, y al menos en lo que refiere a la malla jurídica propia de los "datos personales" no existirá conflicto o impedimento a los efectos de brindar la información solicitada, puesto que aquellos datos, si bien de naturaleza personal, resultan ser especies que escapan al ámbito objetivo de la LPDP, y por tal razón no existirá impedimento en brindarlos.
El tercer y cuarto caso son los que en verdad presentan serias dificultades interpretativas en cuanto a la aplicación del art. 12 de la Ley de Acceso, de modo armónico con las normas provenientes de la LPDP.
En el tercer caso (datos personales ingresados sin necesidad de consentimiento del titular) podemos llegar a admitir que la dificultad o conflictointerpretativo antes señalado se atenúa, aunque no al punto de desaparecer totalmente.
Esta atenuación deriva de la existencia de una relación de proporcionalidad inversa entre el aligeramiento de los postulados tuitivos en materia de protección de datos personales (en este caso por prescindencia del consentimiento del titular) y el aumento de posibilidades de acceso a los mismos. Este tipo de datos pasa a convertirse, así, poco menos que en "res comunii". Sin embargo esta flexibilidad no puede llevar a sostener la inaplicabilidad del resto de postulados contemplados en la LPDP aún a este tipo de datos personales, que solamente escapan al requisito del consentimiento del titular (y sus consecuencias naturales y lógicas, podríamos sostener por extensión), no así a otros requisitos legales como son, entre otros, los principios de legalidad (art. 6 de la LPDP), finalidad (art. 8 de la LPDP) y seguridad de los datos (art. 10 de la LPDP), entre otros.
Finalmente en el cuarto caso, nos enfrentamos a la hipótesis de datos personales protegidos en toda su extensión, sean o no datos sensibles. Es la hipótesis más delicada en cuanto a armonizar el alcance del art. 12 de la Ley de Acceso con el régimen tuitivo de protección de datos personales. A ella consagraremos el resto del informe.

II – Legitimación pasiva: sujetos obligados a brindar información

El art. 12 de la Ley de Acceso pone esta obligación a cargo de "los sujetos obligados por esta ley"**.**
De acuerdo al art. 2 de la misma ley, "información pública" es la que emana o está en posesión de "cualquier organismo público, sea o no estatal...".
Similar solución es sostenida por el Comité Jurídico Interamericano, perteneciente a la Comisión Interamericana de Derechos Humanos en su informe AG./RES 2288 (XXXVII – 0/07) relativo al Acceso a la Información[1] el cual dispone: " *la* ***legitimación pasiva*** *es la obligación del Estado de entregar la información requerida. Esta debe ser amplia e implica que el deber de otorgar la información requerida debe abarcar todo tipo de órganos y autoridades públicas; y los organismos internacionales, las organizaciones intergubernamentales y no-gubernamentales que presten servicios públicos, utilicen fondos públicos o manejen información de interés*

1 Recomendación sobre Acceso a la Información dictada entre otros, por el Comité Jurídico Interamericano. AG/RES. (XXXVII-0/07)

público deben responder a las solicitudes de información y hacer de los principios de publicidad y transparencia materia corriente en su actuar".
En concordancia con lo expresado, quedan excluidos del ámbito de este artículo los supuestos donde el sujeto que recibe la solicitud de información sea un particular o una entidad privada, ya que en estos casos no estaríamos dentro del ámbito de la información publica.
Podríamos hacer un aporte más a este criterio diciendo que en la discusión parlamentaria sobre la Ley de Acceso, al abordarse el artículo 12 se emplea el término "jerarca", que bajo una interpretación literal de este capítulo del Informe es dable concluir que se utiliza generalmente cuando se habla de Órganos estatales.

III – Legitimación activa: sujetos facultados a solicitar información

En este punto el art. 12 de la Ley 18.381 no contiene previsión expresa, debiéndonos remitir a los arts. 3 y 13 de la misma ley de los que se desprende una legitimación amplia y sin restricciones: "todas las personas", "toda persona física o jurídica interesada".
Se trata de un derecho que se ejerce "sin justificar las razones por las que se solicita la información" (art. 3 de la ley), no obstante lo cual debe ejercitarlo una persona "...interesada" (art. 13 de la ley). He aquí un punto de análisis sobre el que habremos de detenernos en el Informe más adelante, cuando analicemos el concepto de "interés" vinculado al ejercicio del derecho de petición, quién y cómo debe calificar el mismo, así como su íntima conexión con uno de los adjetivos que califican y encuadran el tipo legal del art. 12: el término "relevante".

IV - Ubicación del concepto de Violaciones a los DDHH

La definición y alcances del concepto "violaciones de DDHH" resulta esencial a los efectos del presente Informe. De su debido encuadre dependerá, en alta medida, las posibilidades de armonización exitosa del art. 12 de la Ley de Acceso con el régimen de la LPDP.
Estamos ante un concepto abstracto, o mejor dicho, indeterminado, el cual es preciso delimitar en su alcance a los efectos que el artículo sea aplicado de la mejor forma, sin atentar contra otros derechos.
Para poder delimitar el concepto es preciso citar algunos fragmentos de la Sentencia del 29.07.88 dictada por la Corte Interamericana de Derechos Humanos en el caso " Velazquez Rodriguez".[2]
En primer lugar una referencia al art. 1.1 de la Convención Americana sobre Derechos Humanos, que establece:*" que los Estados partes en esta Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que este sujeta a su jurisdicción...".*
En el caso " Velazquez Rodriguez" se afirma que *: " el artículo precedente pone a cargo de los Estados partes los deberes fundamentales de respeto y garantía, de tal*

2 Caso " Velazquez Rodriguez" Sentencia Nº 29 VIII. 1988 Corte Interamericana de Derechos Humanos.

modo que todo menoscabo a los derechos humanos reconocidos por esta Convención, que pueda ser atribuído por las reglas de Derecho Internacional, a ***la acción u omisión de cualquier autoridad pública, constituye un hecho imputable al Estado*** *que compromete su responsabilidad en los términos previstos por la misma Convención"*

Atento a lo mencionado precedentemente entendemos que, para encontrarnos dentro del ámbito de aplicación del artículo en análisis, debe ser el Estado -y no un particular o entidad privada- el sujeto al que se le imputa la violación cuya información se pretende, por virtud de su obligación a someterse a los instrumentos internacionales que ratificó. La Convención Americana de Derechos Humanos establece que ésta se viola en toda situación en la cual el poder público es utilizado para lesionar los derechos humanos en ella reconocidos.

Por lo tanto siempre que estemos ante violaciones de derechos humanos cometidas por el Estado estaremos dentro del ámbito de aplicación del art.12 de la Ley de Acceso. No así en otro tipo de situaciones. Esto descarta todo acontecer donde la información requerida refiera a situaciones en que presuntamente hayan sido los particulares los que cometieron una violación a los derechos humanos. En estos casos se deberán seguir los procedimientos judiciales ordinarios. Creemos que esta fue la intención al sancionar el artículo, y la mejor solución para que este artículo no sirva como válvula de escape para presentar solicitudes de información ante cualquier violación de los derechos humanos, proveniente de agentes privados.

V – Calificación de la solicitud de información

En nuestro concepto, la inexigibilidad legal de justificación de razones para solicitar la información (art. 3 de la Ley de Acceso) no debe llevar a la conclusión apresurada de que el legislador haya querido, a través de esta norma, franquear todo pedido de información atinente a la materia del art. 12, provenga de quien provenga, y cualquiera sea su contenido.

Cuando se trata de solicitudes de información referidas a violaciones de DDHH, entendemos que procede realizar por parte del jerarca un juicio de calificación sobre el interés de quien practica la solicitud. Juicio que no requiere contemplar la existencia de "razones" por parte del solicitante (el art. 3 inhibe tal exigencia), pero sí debe apuntar a constatar otro tipo de elementos connaturales a cualquier acto jurídico, tales como que el solicitante sea persona capaz y posea algún tipo de interés o vínculo con lo que solicita. Juicio amplio y generoso, pero juicio al fin. Recién superado este juicio calificatorio con éxito, habrá de brindarse la información requerida con levantamiento de las reservas existentes en su caso.

Entendemos que esta conclusión anticipada configura el verdadero núcleo del presente Informe, y se impone como único camino de ponderar (el *balancing* de la doctrina anglosajona) los diferentes derechos en juego: acceso a la información vs. protección de datos personales. El mismo esquema de razonamiento procede para aquellos casos en que el primero de los enunciados derechos debiera ser ponderado con relación a otro tipo de derechos diferentes a la protección de da-

tos personales, a efectos de llegar a levantar cualesquiera de las restantes reservas establecidas en el articulado al que remite el art. 12 de la Ley de Acceso.
Por lo tanto, si bien la Ley Nº 18.381 de Acceso a la Información Pública dispone en su art. 3 que el derecho a la información es un derecho de todas las personas y se ejerce sin necesidad de justificar las razones por las que se solicita la información, entendemos que al tratarse de información respecto a violaciones de derechos humanos igualmente habrá de apuntarse a un equilibrio de los derechos en juego, siempre respetando la voluntad de legislador -que por otra parte no recoge más que el enunciado jus-naturalista de la materia- en cuanto a dotar de marcada preferencia al acceso informativo en estos casos, en desmedro de la reserva de los datos personales.
La preferencia anotada no implica necesaria e inexorablemente una eliminación de todo tipo de garantías a favor del derecho desplazado. En todo caso, la restricción de los derechos humanos es calle de doble vía. Dicho de otro modo: los casos concretos dejarán margen para procurar conciliaciones entre derechos en conflicto, y hasta donde sea posible es tarea del jurista y del operador jurídico, lograr estas conciliaciones.
Sobre este punto es destacable lo resaltado por el Dr. Martín Risso quien sostiene que : " *tanto la Constitución como las normas internacionales referidas a los derechos humanos reconocen que algunos derechos deben poder ser objeto, a veces, de limitación o restricción. Y estas limitaciones de los derechos humanos (un acto jurídico de la máxima trascendencia) deben estar rodeadas de las máximas garantías para salvaguardar nada menos que dichos derechos humanos".*[3]
Entre las garantías suficientes que se tienen que guardar, sería bueno exigir a la persona que solicita la información un interés legítimo entendido éste como vínculo siquiera genérico (pero siempre existente, pertinente y lícito) con lo que cabe esperar sea el tratamiento o difusión posteriores de este tipo de informaciones. De esta forma evitamos que una persona que no tenga un interés comprobable, y que por ende no se sienta afectado por la información, pueda no obstante acceder a la misma, y en última instancia se termina impidiendo la violación de un derecho, como es el de la protección de datos personales, derivado del derecho fundamental a la intimidad, de rango constitucional.
La doctrina estudia y califica los tipos de interés presentes en el ejercicio de peticiones ante el Estado. Citando a GUICCIARDI, DURÁN MARTÍNEZ expresa que cualquier persona podría alegar su interés en que se cumplan las normas sobre organización, contenido o procedimientos (normas que por definición carecen de un correspectivo derecho subjetivo). Pero en tal caso, sostiene el autor, "ese sería un interés considerado vago o impreciso que por no estar especialmente protegido por el ordenamiento jurídico se denomina interés simple o mero interés". Y a renglón seguido, el mismo autor expresa "que puede ocurrir que existan sujetos respecto de los cuales el cumplimiento o no de esas normas de acción por parte de la Administración los afecte de modo particular con relación a otros..."

3 RISSO FERRAND, Martín " Primeras reflexiones sobre el Proyecto de Reforma Constitucional a plebicitarse en Octubre de 2004

calificando al interés en juego, en este caso, como "interés legítimo".[4]
En nuestro régimen jurídico positivo de protección de datos contenido en la LPDP es interesante advertir lo que reza el art. 17; " *los datos personales objeto de tratamiento solo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el* ***interés legítimo*** *del emisor y el destinatario (...) al titular de los datos se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo".*
Según surge precedentemente el art. 17 de la LPDP habla de "interés legítimo" del destinatario de datos y la propia ley se encarga de definir el concepto de destinatario de datos como aquella *"persona física o jurídica, pública o privada, que recibiere comunicación de datos, se trate o no de un tercero"*. Por lo que de dichas disposiciones normativas surge claramente la necesidad del interés legítimo del solicitante de información, explicitable de modo minimalista, en función de las atenuaciones y prevalencias que surgen del régimen jurídico de "acceso a la información pública", en especial de los arts. 3 y 12 de la ley.
En el derecho argentino resulta relevante agregar lo sostenido en el dictamen Nº 38/08 de la DNPDP[5]. Ésta sostiene, basándose en una disposición contenida en la Ley Nº 25.326 (muy similar a la del art. 17 de la LPDP), que : " *en consecuencia, exigiendo la Ley Nº 25.326 la existencia de interés legítimo, los datos personales no podrían cederse frente a la ausencia en el caso concreto de ese interés (...) ello es así por cuanto* ***el interés legítimo es lo que determina la licitud del tratamiento de datos personales****. De modo que, no solo la finalidad de la base de datos debe ser legítima sino que la cesión de datos solo puede hacerse para el cumplimiento de los fines relacionados con los intereses legítimos del cedente y cesionario. Es una manera de hacer respetar el principio de finalidad para que los datos que fueron recogidos para un fin no sean destinados a otro".*
El precitado dictamen continua sosteniendo que además de acreditarse el interés legítimo, debería también evaluarse el tipo de información de que se trata, y nosotros agregamos, *a fortiori*, que tratándose de temas relativos a violaciones a los derechos humanos, donde al tiempo que se accede a cierto tipo de información emerge paralelamente una concreta posibilidad de lesionar el derecho a la intimidad, la constatación de un interés del solicitante, en los términos y alcances anotados en el presente Informe, se hace tanto más necesario a los efectos de lograr un equilibrio de los derechos constitucionales en juego.
No nos parece que exigiendo un interés legítimo estemos contrariando la Ley de Acceso a la Información Pública, ya que en supuestos de violaciones a los derechos humanos, situaciones rodeadas de mucha fragilidad, con frecuencia serán los herederos universales quienes soliciten este tipo de información, estando correctamente legitimados para ello (art. 14 inc. 2 LPDP). Claro está que otro tipo de requirentes, como pueden ser las organizaciones defensoras de DD.HH. o los periodistas, merecerán un juicio calificatorio posiblemente más detenido y estricto, en tanto vía de preservar el equilibrio del sistema en su conjunto.

4 DURAN MARTINEZ, Augusto - "Contencioso Administrativo", pág. 110.
5 Dictamen dictado por la Dirección de Protección de Datos Personales (Argentina) Nº 38/08 del 28 de Noviembre de 2008.

En el ámbito de las Organizaciones de DDHH se movilizan numerosas instituciones entre las cuales están las ONG, como organizaciones no gubernamentales, que entre otros cometidos tienen los de implementar políticas de tutela de los DDHH, con intervenciones de variado alcance en la sociedad.
En cuanto al análisis de si es necesario que este interés sea directo, y en virtud de armonizar la Ley de Acceso con la LPDP, entendemos que nos encontramos en los lindes de lo que procede legalmente exigir, a la luz de un régimen jurídico de acceso a este tipo de informaciones, en el que se privilegia no justificar razones para la solicitud de información (art. 3 Ley de Acceso). Pero de ahí a admitir la mera presencia de intereses vagos o no explícitos como suficientes para solicitar este tipo de informes, nos parece que la respuesta debe ser negativa. Nos ratificamos una vez más, en que existe -como ya se dijo- un terreno propio a la calificación de ese interés por parte de quien debe brindar la información.
Si se quiere sumar argumentos de texto para la exigencia de un "interés" de parte del solicitante de informaciones referidas a DDHH, los encontraremos en la propia Ley 18.381. Los arts. 13 y 14 refieren, respectivamente a "persona interesada" y a "peticionarios", categorías ambas que suponen la presencia de un interés legítimo (cf. DURAN MARTÍNEZ op. cit.). Por lo que será acorde exigir por parte del jerarca que el solicitante acredite dicho interés, el que a juicio de los informantes debe traducirse en una necesidad imperiosa, urgente, en cuanto a tener que averiguar acerca de la presunta violación de los derechos humanos en desmedro cierto de la preservación de los datos personales contenidos en la misma. Este criterio se afinca en la necesidad de explicitar requisitos o condiciones de operabilidad de las restricciones a los DDHH dentro de una sociedad democrática, y en tal caso exigir que nos encontremos ante situaciones imperiosas, que justifiquen la interferencia o abatimiento de un derecho en procura o favor del otro.
Como expresáramos anteriormente, siempre se estará frente a casos concretos donde no siempre todas las variables operarán con la misma fuerza y alcance, y donde el organismo que reciba la solicitud de información habrá de realizar su propio juicio al respecto. En caso de negarla, será el juez quien atendiendo también las circunstancias concretas sometidas a su juicio, habrá de realizar una adecuada ponderación de los derechos en juego.

VI – El concepto de información "relevante"

Otro aspecto a destacar acerca del ámbito de aplicación de éste artículo, es el término "relevante" para calificar el libramiento de información previsto por el art. 12 de la Ley de Acceso.
Según el diccionario de la Real Academia Española algo relevante, es algo sobresaliente, significativo, destacado.
El término "relevante" se refiere, así, a que la información sobre violaciones de derechos humanos debe ser significativa. Por lo que en los casos en que se solicite el acceso a este tipo de información, el jerarca debe analizar el contenido de la información solicitada, y observar su importancia. Esto es necesario para evitar que se haga un uso abusivo del artículo, y que en caso de accederse a la informa-

ción con relego del derecho de protección de datos personales como lo quiere el legislador, sea en verdad por encontrarnos ante una situación que justifique tal relego.
En los casos en que el jerarca considere que la información no posee el carácter de "relevante", será el juez quien deba analizar el caso concreto y determinar si amerita el derecho al acceso a la información en las condiciones planteadas.
En este supuesto es menester agregar que en la discusión parlamentaria sobre la Ley de Acceso se afirmó que el jerarca siempre tiene la posibilidad (y sería de buen proceder que así lo hiciera) de realizar una consulta al Órgano de Control el cual podrá a su vez, solicitar al Consejo Consultivo se expida sobre el punto, en aquellos casos en que exista la duda de si se trata o no de violaciones de derechos humanos (Literal "G" art. 21 de la Ley de Acceso).
Esta práctica permitirá salvaguardar el derecho a la intimidad del titular de los datos objeto de la consulta. Abona un mayor fundamento a esta tesitura el concepto mismo de violaciones de derechos humanos, el cual es de tipo abstracto y debe acotarse a supuestos contenidos en los tratados internacionales suscriptos por Uruguay. Será dentro de ese marco normativo, y evaluando el caso concreto, que el juez podrá realizar una adecuada ponderación de los derechos en juego.
Atendiendo este tipo de circunstancias fue que, en la discusión parlamentaria sobre la Ley de Acceso, se estableció que: " presentada una solicitud acerca de información sobre Derechos Humanos, si el jerarca considera que debe ser denegada por no tratarse de este caso particular, se abre la instancia judicial prevista en el artículo 22". Este antecedente apoya nuestra interpretación acerca de que, en los casos de presuntas violaciones de derechos humanos, el jerarca debe analizar la solicitud presentada y la relevancia de la información, así como, de no proceder, podrá denegarla y abrirse la instancia judicial prevista en la Ley de Acceso.
Antes de abordar el siguiente punto agregamos que cuando se solicita información circunscripta en el ámbito del art. 12 de la Ley de Acceso, el principio o regla de base es que no se debe revelar, bajo ninguna razón, datos personales de terceras personas, aunque se vinculen con los datos personales del titular, ya que los datos personales de terceras personas están protegidos en toda su extensión por la LPDP.

VII - Cumplimiento de los Principios referentes a la Protección de Datos Personales

El régimen positivo de la protección de datos se nutre de varios principios funcionales al propósito de salvaguardar los datos personales y hacer un uso correcto de éstos, apuntando siempre a tutelar al titular de los datos. Con diversos grados de tuición, se entiende que el conocimiento público de ciertos datos protegidos por la legislación actual puede convertirse en una amenaza para el individuo y su reputación, así como también su entorno familiar y social.
DELPIAZZO afirma que abonan la confidencialidad de la información de carácter personal - erigida ella misma como principio general un conjunto de principios

generales de Derecho, que con distintos grados de explicitación son reconocidos en el derecho comparado.[6]

En la LPDP se encuentran recogidos algunos de estos principios, entre otros el Principio de Veracidad, el Principio de Finalidad.

Sin hacer referencia a cada principio en particular -lo que excedería el propósito de este informe- e interpretando la LPDP, arribamos a la siguiente conclusión: en casos de que se solicite información en el ámbito del artículo 12 de la Ley de Acceso, el jerarca deberá analizar (además del interés legítimo del solicitante) primero si se trata de violaciones a los derechos humanos, segundo si posee relevancia, y tercero en los casos donde conceda el acceso deberá siempre aplicar los principios contenidos en el régimen de protección de datos. Esto es, deberá proporcionar la información de manera ecuánime, no excesiva y en relación a al finalidad para la cual fueron solicitados.

Además, en virtud del artículo 17 de la LPDP, en los casos de comunicación de datos se deberá informar al titular acerca de la finalidad de la comunicación, e identificar al destinatario. Recordar que el destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor, y éste responderá solidaria y conjuntamente por la observancia de dichas obligaciones ante el organismo de control y el titular de datos de que se trate. Al respecto existe la misma solución en el derecho argentino, en el ya citado Dictamen 38/8, con referencia a las responsabilidades del cedente y cesionario de los datos, la cual será solidaria, y agrega el dictamen: *"el cesionario deberá observar el deber de confidencialidad".*

La solución anteriormente explicitada está en la misma línea del artículo 13 del Pacto de San José de Costa Rica, que al referirse a la Libertad de Pensamiento y Expresión establece: *"...este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole..." y continua diciendo : "el ejercicio de este derecho no puede estar sujeto a censura, sino a* ***responsabilidades ulteriores****, las que deberán estar expresamente fijadas por la ley y ser necesarias para asegurar: a) el respeto a los derechos o a la reputación de los demás...".*

Por lo tanto, relacionando la LPDP y el Pacto de San José de Costa Rica y entendiendo al derecho de acceso a la información como desprendimiento o parte de la libertad de información (referencia que profundizaremos mas adelante), llegamos a la conclusión de que, a los efectos que el jerarca acceda a conceder la información solicitada, se deberán seguir los pasos ya enunciados, y se deberán determinar las responsabilidades ulteriores de la comunicación de los datos personales de parte del destinatario de la información.

De esta manera, además de seguir en concordancia con el régimen tuitivo de la protección de datos personales, evitamos que ante el ejercicio del derecho al acceso a la información se deje de lado una efectiva ponderación de otros derechos identificados con el tema en análisis.

Finalmente hacemos nuevamente una referencia a la opinión de DELPIAZZO hablando de los principios generales del derecho. El autor afirma que éstos son pilares de todo ordenamiento jurídico, estructurados no sólo en el mundo real

6 DELPIAZZO, Carlos " A la búsqueda del Equilibrio entre Privacidad y Acceso" Pág. 7 y sigs.

sino también en el espacio de relaciones conocido bajo el nombre de "ciberespacio", y resultan de directa aplicación al mismo. Es así que para el citado autor, en el ámbito del ciberespacio adquiere relevancia el Principio Protector.
Este principio protector, según el autor, está referido al derecho a la intimidad de cada persona, y se constituye en un límite al ejercicio de derechos tales como el de información, cuando pueda plantearse un conflicto entre tales derechos.[7]

VIII - El Derecho a la Intimidad y el Derecho al Acceso

En primer lugar vamos a centrarnos en la normativa aplicable, para luego hacer algunas consideraciones sobre el tema.
Con respecto a la normativa existente, tenemos la Declaración Americana de los Derechos y Deberes del Hombre y el Pacto de San José de Costa Rica entre otros.
La Declaración Americana de los Derechos y Deberes del Hombre en su artículo 5 establece: "*Toda persona tiene derecho a la protección de la ley contra los ataques abusivo a su honra, a su reputación y a su vida privada y familiar".*
Por su parte el Pacto de San José de Costa Rica precedentemente citado, nos remite a las conocidas "tres libertades" en materia de información, y al principio de responsabilidad ulterior (no censura previa).
Cuando analizamos el artículo 12 de la Ley de Acceso desde el punto de vista de la protección de datos personales debemos prestar atención especialmente a los efectos negativos que el ejercicio del acceso a la información tenga sobre el régimen tuitivo de la protección de datos personales. Para ello debemos concentrarnos en los derechos protegidos por ambos.
DELPIAZZO afirma que la protección de datos es el nuevo rostro del derecho a al intimidad, convencido de que se trata de una emanación de aquél con independencia actual de su fuente original.
En efecto, la intimidad refiere al conjunto de características biológicas, psicológicas, éticas, espirituales, socioeconómicas y biográficas de una persona, que forman parte de su vivencia o conciencia, comprendiendo no sólo el ámbito mínimo del individuo consigo mismo (el derecho a estar solo) sino también lo que el individuo realiza en su hogar, fuera de la vista de los demás, y aún los hechos y circunstancias que, aunque se desarrollen en lugares públicos o puedan ser observados por otros, la persona no tiene interés en que se propaguen.[8]
En efecto, con el surgimiento de las nuevas tecnologías este derecho a la intimidad es atacado con un grado de mayor agresividad, por lo que se trata de proteger no solamente el derecho a la intimidad sino la esfera de mayor alcance que constituye la privacidad de la persona.
Por otra parte en la Ley Española 30/92 se establece como limitación al derecho al acceso, el derecho de la intimidad de las personas, y además se establece que la Administración podrá negarse a proporcionar los datos personales cuando existan intereses de terceros más dignos de protección.[9]

7 DELPIAZZO, Carlos y VIEGA, María José " Lecciones de Derecho Telemático"
8 DELPIAZZO, Carlos "A la búsqueda del Equilibrio entre Privacidad y Acceso" pág. 7 y Sigs.
9 Ley Española 30/92 que regula el régimen jurídico de las Administraciones Públicas y del

Siguiendo la intelección de las normas anteriormente mencionadas, estamos en condiciones de afirmar que es necesario delimitar el ámbito de aplicación del artículo 12 de la Ley de Acceso.

En primer lugar es importante tener en cuenta, que en cada oportunidad que estemos ante la aplicación de este artículo se tendrán que tomar las medidas necesarias para proteger la privacidad de las personas, ya que como afirma la Convención Americana de los Derechos y Deberes del Hombre: la ley debe proteger contra el abuso de la vida privada y familiar del individuo, y por analogía a los efectos de este Informe, al titular de los datos personales.

Nuestro ordenamiento positivo no contiene la limitación existente en la legislación española, en la cual el derecho al acceso a la información no puede ejercerse cuando los datos se refieran a la intimidad de las personas. Si bien estamos ante supuestos de violaciones a los DDHH consideramos que se debe establecer parámetros para poder proteger el derecho a la intimidad de los titulares de los datos. Siempre intentando aplicar armónicamente las dos legislaciones vigentes.

El Pacto de San José de Costa Rica, ratificado por Uruguay por Ley Nº 15.737 se refiere en su artículo 13 a la libertad de pensamiento y expresión.

Del derecho de la libertad de expresión se desprende la libertad de información conceptuada bajo imperativos de actualidad, como aquella modalidad de la libertad de expresión que se realiza por o a través del cauce de las modernas tecnologías. Y consecuentemente a esta evolución histórica signada por varios paradigmas de creciente presencia en la sociedad (globalización, aumento de las comunicaciones por medio de múltiples tecnologías, etc.), del derecho a la información se desprende también el derecho al acceso a la información pública, el cual emerge con plena autonomía de éste.

Ahora bien, el artículo 13 establece que el ejercicio del derecho de libre expresión esta sujeto a responsabilidades ulteriores, las que se deben establecer por ley y ser necesarias para asegurar el respeto a los derechos o a la reputación de los demás.

Como bien señala DELPIAZZO el derecho al acceso a la información pública se basa, entre otros, en el principio de publicidad de la información mientras que la información privada (la que comprende datos que tienen que ver con la intimidad de la persona, y su conocimiento puede llegar a ser una amenaza para el individuo) se basa en la reserva y en el principio de confidencialidad. A la luz de estas consideraciones que se acaban de exponer, se desprenden otros principios comprendidos en el marco normativo de la LPDP, como son el principio de justificación o finalidad, veracidad, limitación de la recolección, entre otros.[10]

Atento a lo expuesto consideramos, basándonos en la normativa internacional que en los casos en que deba aplicarse el artículo 12 de la Ley de Acceso, y el jerarca acceda a la solicitud, se deberán implementar medidas administrativas y establecerse responsabilidades a los efectos de salvaguardar la intimidad y pri-

Procedimiento Administrativo

10 Seminario de Habeas Data en Uruguay. : " A propósito del Acceso a la Información pública" Ponencia expuesta por el Dr. Carlos Delpiazzo.

vacidad de las personas titulares de los datos personales . Es de esta forma que la puesta en práctica del artículo no afectará un derecho establecido constitucionalmente, como es el derecho a la intimidad, no contradiciendo tampoco el Pacto de San José de Costa Rica.

IX - Ponderación de los Derechos a la Intimidad y del Acceso a la Información

A lo largo del presente Informe hemos explicitado que su objetivo es lograr establecer ciertos parámetros a los efectos de, frente al caso concreto, realizar una adecuada ponderación de los derechos.
El trabajo de ponderación (*balancing* en la literatura especializada anglosajona) puede pensarse como la tarea racional de jerarcas y jueces en la búsqueda de compensación o equilibrio entre dos pesos, o el balanceo de razones para la decisión jurídica. Se trata de operaciones que se practican cuando hay concurrencia de soluciones jurídicas frente a un mismo caso; expresadas como un conflicto entre principios, reglas o valores, para el cual el ordenamiento no prevé una solución o no puede preverla. Corresponde por ello al operador jurídico establecer la solución a seguir.[11]
ALEXY entiende que la ponderación se deriva de la naturaleza de los principios vinculada a los derechos de cada caso, y la asimila a un principio de proporcionalidad. El juicio de proporcionalidad toma en cuenta tres criterios o sub principios: *idoneidad* (*suitability*), para lo cual la restricción debe ser adecuada al fin protector que se defiende; *necesidad* entendida como el *empleo del medio menos lesivo para los derechos,* y en tercer término la *proporcionalidad en su sentido estricto, es decir, el requerimiento de balanceo como medio para apreciar beneficios y pérdidas de los diferentes derechos en disputa.*[12]
DELPIAZZO ha analizado muy bien el tema de la ponderación de los derechos al acceso y el derecho a la protección de datos personales, y por ende nos remitimos a su trabajo, citando algunos pasajes del mismo.

(...) "partiendo de la necesaria interpretación armónica de los derechos, impuesta no sólo por la unidad del sujeto humano, sino también por la regla general de interpretación constitucional sistemática, en casos de concurrencia de derechos, la labor del intérprete debe centrarse en pensar cada uno de los derechos en juego desde su contenido esencial, a efectos de determinar, no el "peso" concreto de los mismos para apreciar cuál es más importante o cuál debe rendirse, sino cuál de ellos comparece y cuál no en el caso concreto".

(...) *"***En el caso particular***, el equilibrio entre el derecho a la información (y su desprendimiento, el derecho de acceso a la información pública) por una parte, y el derecho a la protección de datos personales (ubicado concéntricamente con los dere-*

11 SANCHEZ FERNANDEZ, Luis Manuel " Ponderación y Casos Difíciles en Materia Constitucional " Pág. 53
12 ALEXY R. " A Theory of Constitucional Rights p.102

chos a la intimidad y a la privacidad) por otra parte, aboga a favor de este último cuando existen datos personales en poder de la Administración susceptibles de ser accedidos no sólo por el titular sino por terceros".

(...) "Si el ejercicio de un derecho afecta la consecución de la finalidad de otro, entonces habrá que examinar si la finalidad que persigue el primero se encuentra en correspondencia con la finalidad que persigue el segundo. En la especie, es evidente que el ejercicio del derecho de acceso a la información pública, si no respeta el límite de la información privada, desvirtúa su fin. A su vez, la reserva de los datos personales no afecta el contenido esencial del derecho de acceso a los documentos administrativos."[13]

Como nuestro ordenamiento jurídico no prevé una solución en caso de ponderación de los derechos de la protección de datos y el derecho a la información pública, debemos estar siempre al caso concreto, y el juez tendrá la difícil tarea de tomar las medidas necesarias y analizar en cada caso particular, las circunstancias enunciadas a lo largo de este Informe: el interés legítimo del solicitante, si estamos verdaderamente ante información calificada dentro de los supuestos del art.12 de la Ley de Acceso, el cumplimiento de los principios de la LPDP hasta donde sea posible, así como también los supuestos y características particulares de los derechos de protección de datos y acceso a la información pública puestos en clave interpretativa de balance entre unos y otros. Y por último el magistrado tendrá la difícil tarea de ponderar uno de los dos derechos, con la consecuencia lógica -pero minimizada al máximo posible- de restringir al otro.
Atento a ésto, consideramos de buen proceder que el Estado como suscriptor de la Convención Interamericana de Derechos Humanos, en la medida que comenzaren a plantearse situaciones ubicables en el ámbito del art.12 de la Ley de Acceso, solicite opiniones consultivas a la Corte Interamericana de Derechos Humanos. Se trata de actos, si bien, no vinculantes, que poseen relevancia significativa en temas relativos a los derechos humanos, y además estaría colaborando en el mejor desarrollo de los derechos humanos que puedan ser vulnerados en virtud de un uso abusivo del artículo en análisis.

X – ¿Inconstitucionalidad del Art. 12?

La inoponibilidad o no vigencia de uno de los principios jurídicos fundamentales en materia de protección de datos personales, como es el de "reserva" (del cual depende en práctica y gran medida la sustentabilidad del régimen en su conjunto), en los supuestos consagrados por el art. 12 de la Ley de Acceso, hace necesario analizar la eventual inconstitucionalidad de este artículo.
El derecho de la protección de datos personales es un derecho fundamental de rango constitucional a texto implícito (art. 72 de la Constitución), que el referido art. 12 vendría a conculcar. La pregunta que nace inmediatamente es si la norma en cuestión, de rango legal, puede abatir un derecho de la

13 DELPIAZZO, Carlos " A la Búsqueda del Equilibrio entre la Privacidad y el Acceso pág. 14

personalidad, de origen constitucional.
Según ALEXY las "restricciones, para ser tales, deben ser constitucionales, si no son intervenciones arbitrarias". Y continúa precisando el mismo autor: "las restricciones de los derechos humanos son, entonces, normas de rango constitucional, o bien normas de rango inferior a la Constitución, mediante autorización que da la Constitución, de dictar normas restrictivas de los derechos humanos".
Siguiendo el mismo razonamiento, "es perfectamente viable la regulación de un derecho humano mediante la ley, y éste no debe entenderse como restricción, al menos cuando de esta regulación se desprenda alguna verdadera limitación del derecho en cuestión, establecida o autorizada por la Constitución, en virtud de los derechos de las demás personas".[14]
Nuestra Carta Magna permite el recorte o limitación de los derechos fundamentales por "leyes de interés general", al tenor de su art. 7. Sin embargo, la redacción drástica del art. 12 de la Ley de Acceso, estableciendo un mandato imperativo de fuertes repercusiones (vg. "...no podrán invocar ninguna de las reservas mencionadas en los artículos que anteceden") nos enfrenta a la disyuntiva de considerarlo, o bien como una hipótesis limitativa encuadrada dentro de la norma constitucional que así lo habilita, o bien como una norma inconstitucional si no se diera este posible encuadre.

XI - Conclusiones Finales

1) El presente informe pretende ser un aporte a los efectos de ofrecer ciertas pautas que permitan analizar en cada caso concreto que se presentase, el conflicto del art. 12 de la Ley de Acceso con el régimen de la LPDP, y las eventuales soluciones al mismo.

2) En cuanto a la legitimación pasiva, o sea quienes son sujetos obligados a brindar información referente a violaciones de derechos humanos, ésta comprende en el marco de la Ley de Acceso a todo organismo público, sea o no estatal, así como también a otras organizaciones internacionales o intergubernamentales como lo explicita la recomendación del Comité Jurídico Interamericano.

3) En cuanto a la legitimación activa, sugerimos que en los casos donde haya de aplicarse el art. 12 de la Ley de Acceso, se exija por parte del jerarca, la acreditación de un interés legítimo del solicitante. Exigencia que apunta al objetivo de garantizar el derecho de la protección de datos personales, la privacidad y reputación del sujeto objeto de investigación y evitar una aplicación abusiva de la disposición en análisis.

4) El término "violaciones a los derechos humanos" refiere a todo menoscabo que se haga de éstos por parte del Estado, o cuando el poder público sea utilizado para lesionarlos, excluyéndose del ámbito de la norma las violaciones

14 Cit. por FUENMAYOR CHACIN, Ronald de J. - "La doctrina de interpretación de los Derechos Humanos y la Constitución Venezolana de 1999", págs. 9 y 10.

por particulares o entidades privadas. La solución es acorde con lo dispuesto por la Convención Americana de Derechos Humanos, y creemos que fue esa, y no otra, la intención del legislador al sancionar el artículo en cuestión.

5) Tratándose de solicitudes en las que el jerarca proceda a brindar la información, se deberá guardar respeto a los principios imperantes en materia de protección de datos personales en el grado máximo posible, poniendo resguardo y advertencia al destinatario de los datos, en cuanto al hecho de que tendrá las mismas responsabilidades que el responsable del tratamiento de éstos.

6) El derecho a la protección de datos derivado del derecho a la intimidad, y el derecho al acceso a al información derivado del derecho a la información, deben ser evaluados en cada caso concreto que se presentare, siempre teniendo en cuenta la finalidad de cada uno, su contenido esencial y los términos de prevalencia en cada caso.

7) Dada la trascendencia del conflicto que plantea el art. 12 de la Ley de Acceso, se sugiere tener presente la posibilidad de solicitar opiniones técnicas a título consultivo dirigidas al Consejo Consultivo de la Unidad de Acceso a la Información, y en su caso -a nivel estatal- a la Corte Interamericana de Derechos Humanos, ambas posibilidades previstas por el régimen de la materia.

Firmado por Dr. Federico Carnikian - Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 19 de 22 de mayo de 2009.- Se informa sobre consulta referida a la legalidad de las llamadas realizadas con fines políticos

Montevideo, 22 de mayo de 2009

Informe Nº 19
Exp. 015/2009
Ref. Consulta sobre legalidad de las llamadas realizadas con fines políticos

Antecedentes

La consulta formulada por el Sr. Eduardo Delgado de la empresa periodística "El País" acerca de si está permitido o viola alguna normativa vigente la práctica de grupos políticos que realizan llamadas telefónicas a números fijos o de celulares, divulgando actividades de los precandidatos y dirigentes políticos que las apoyan.

Analisis

I) Se trata de una práctica publicitaria constatada en nuestro medio, a partir de las respectivas campañas de candidatos a las elecciones internas de los partidos políticos.
Esta práctica podría estar efectivamente violando el régimen jurídico de protección de datos personales, vigente con carácter general a partir de la Ley 18.331 promulgada el 11 de agosto de 2008, publicada en el Diario Oficial No. 27549 del 18 de agosto de 2008, dependiendo ello de diferentes alternativas con la que pudiera estar operando en los hechos.

II) La Ley de Protección de Datos y Acción de "Habeas Data" No. 18.331 define en su art. 4o. Literal E el "dato personal" como la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. En consecuencia, los números de teléfono celular y teléfono fijo de personas físicas o jurídicas, tienen la calidad de datos personales en tanto identifiquen, o puedan hacerlo, a sus titulares.

Del elenco de previsiones jurídicas contempladas por la ley para la utilización y tratamiento legítimo de este tipo de datos, se destacan a los efectos de la presente consulta las siguientes:
A) La prestación de consentimiento libre, previo, expreso, informado y documentado del titular, a los efectos del tratamiento legítimo de sus datos (art. 9 de la Ley).
B) La comunicación a terceros con el mismo requisito del consentimiento, más la

información al titular sobre la finalidad de la comunicción y la identificación del destinatario (art. 17 de la Ley).

III) En caso de contar con el consentimiento directo del titular involucrado, el régimen legal establece de todos modos algunas excepciones a la regla, entre las que figura que los datos objeto de tratamiento o comunicación posterior, provengan de fuentes públicas de información, fuente que indudablemente existe en materia de teléfonos fijos a través de la Guía Telefónica (siempre que el usuario no haya solicitad su exclusión), no así en materia de teléfonos celulares (art. 9 literal A de la Ley). Asimismo cabe considerar como excepciones al régimen general del consentimiento del titular, dos hipótesis más, a saber: cuando se trate de la utilización de números telefónicos pertenecientes a personas jurídicas (art. 9 literal C de la Ley); y la posibilidad de apelar al procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables (arts. 4 literal G, 17 literal D).

IV) En síntesis, y no contando el país con una normativa legal que controle o restrinja la publicidad masiva no solicitada por el receptor (a excepción de las normas de este carácter contenidas en la Ley No. 17.250 que no aplican a la especie en consulta), debe concluirse que la práctica objeto de consulta es lícita, bajo ciertos términos o condiciones.

En primer lugar debe distinguirse si esta práctica se realiza con relación a servicios telefónicos pertenecientes a personas físicas o jurídicas. En el primer caso, si no hubo previo consentimiento, o acceso vía una fuente pública al dato del número teléfonico, se concluye que la conducta objeto de consulta es ilícita. En el segundo caso, o sea que el número provenga de listados referentes a personas jurídicas, se estará ante una práctica lícita.

En segundo término se impone distinguir si se trata de llamados a números de telefonía fija, o a números de telefonía celular. En el caso que las llamadas se realicen a teléfonos fijos y provengan de registros públicos como la Guía Telefónica, no se aprecia ilicitud. En cambio, en el caso que las llamadas se realicen a teléfonos celulares, al no existir registros públicos y tratándose de titulares personas físicas, las empresas de telefonía celular no podrán proporcionar listados que incluyan los nombres de los titulares con sus respectivos números, a quienes desarrollan estas prácticas, a no ser que se hubiera dado consentimiento informado previo a este tipo de comunicaciones en los términos del art. 17 de la Ley, lo que en principio no aparece probable.

Finalmente, existe siempre la posibilidad de la disociación de la información de forma tal de hacerla anónima, consistente para el caso en listados que las empresas telefónicas suministrasen a terceros conteniendo exclusivamente números de teléfono, sin conectarlos con ninguna otra clase de información que llevase a determinar sus titulares. Práctica que, en tal hipótesis, será lícita al tenor de los arts. 4 literal G y 17 literal D de la Ley.

V) Sin perjuicio de lo precedentemente expuesto, cabe acotar que existen programas informáticos que llaman en forma aleatoria, generando el número en forma randómica, lo que no constituye una base de datos.

Conclusiones

I) En el estado actual de nuestra legislación, la publicidad electoral masiva a través de teléfonos fijos no violenta el régimen jurídico. En lo que respecta a la competencia de esta Unidad, cuando la difusión se realiza -en el caso de personas físicas- utilizando fuentes públicas de información como la Guía Telefónica, o bien se trata de números pertenecientes a personas jurídicas, resulta legítima.

II) El artículo 21 de la LPDP regula los datos relativos a Bases de Datos con fines de publicidad y dispone 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 figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. Es decir que en el desarrollo de la actividad publicitaria, siempre se requiere, o bien el consentimiento del titular, o bien la información provenga de fuentes accesibles al público, otorgándosele al titular del dato, el derecho de solicitar en cualquier momento su retiro o bloqueo. Por ende, las llamadas que se realicen a teléfonos fijos divulgando cualquier tipo de actividad propagandística o publicitaria, cuyos datos hayan sido facilitados por sus titulares o con su consentimiento, o provengan de registros públicos como lo es la guía telefónica, no resultan violatorias de la ley.

III) Tratándose de difusión practicada a través de teléfonos celulares cuyos titulares sean personas físicas, y en la medida que no existen fuentes de acceso público a este tipo de datos en nuestro país, se estará ante una práctica ilícita en el caso que se estuvieran utilizando informaciones de carácter personal que recaigan sobre personas determinadas o determinables, lo que determina que las empresas de telefonía celular no deben proporcionar listados que incluyan los nombres de los titulares con sus respectivos números, a quienes desarrollan estas prácticas, salvo consentimiento informado previo a este tipo de comunicaciones en los términos del art. 17 de la Ley.

IV) En cualquier caso se considera lícita la posibilidad de disociación de la información de forma tal de hacerla anónima, consistente para el caso en la utilización de listados que las empresas telefónicas cabe que suministren a terceros conteniendo exclusivamente números de teléfono, sin agregados ni conexiones con ninguna otra clase de datos que llevase a determinar los titulares de tales servicios. Sobre el punto, téngase presente, además, lo informado en capítulo V del Análisis.

Firmado por Dr. Marcelo Bauzá-Dra. - Mª José Rodríguez Tadeo
Derechos Ciudadanos

Informe N° 20 de 22 de mayo de 2009.- Se informa sobre aspectos generales de la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data

Montevideo, 22 de mayo de 2009

Informe Nº 20/2009
Exp. Nº 2009/016
Ref. Consulta sobre aspectos generales de la Ley Nº 18.331 de Protección de Datos Personales y Acción de Habeas Data"

Antecedentes

El Semanario "Búsqueda" consulta vía correo electrónico sobre aspectos de la Ley Nº 18.331 de Protección de Datos Personales y Acción de "Habeas Data".
A continuación, responderemos cada una de las interrogantes particulares:

1) *¿Qué tipos de bases de datos tienen que registrar las empresas? (Concretamente me interesaría tener ejemplos prácticos al respecto de acuerdo a distintos tipos de empresas, tamaños y sector de actividad para poder llevar la ley a la "práctica"; ¿compañías de telefonía celular, bancos, tarjetas de crédito, servicios de salud, estudios profesionales, una farmacia que tiene registrada las direcciones de sus clientes, y necesitaría más ejemplos de pequeñas empresa que deban registrarla, etc.?)*

Se deben registrar las bases de datos que contengan "datos personales". Se entiende por datos personales a toda información personal que permita identificar a la persona, o la vuelva identificable. Esta precisión es importante porque, en ocasiones, ciertos datos no identifican de por sí a una persona, mientras que si son utilizados en conjunto sí lo hacen.
El régimen de registro es independiente del tamaño y del sector de actividad, cabe señalar que, por otra parte, la Ley se aplica tanto al ámbito público como privado, por lo que las instituciones públicas también deben registrar sus bases de datos.
La Ley prevé las siguientes excepciones:

- Las bases de datos que pertenecen a personas físicas para su uso personal o doméstico.
- Las bases de datos utilizadas por el Estado para finalidades relativas a la seguridad pública, la defensa nacional, las actividades en materia penal y represión del delito.
- Las bases de datos creadas y reguladas por alguna Ley especial.

2) *¿Cuáles son los principales cambios que se introducen para las empresas en lo que tiene que ver con la gestión de las bases de datos? (también en este caso me interesa poder mencionar algunos ejemplos)*

Los cambios surgen a partir de los principios de la ley, que se plasman en derechos de los titulares de los datos y obligaciones por parte de las instituciones responsables de las bases de datos.
Vale la pena enumerar esos principios: legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad.
Estos principios, en su aplicación cotidiana, se reflejan las siguientes situaciones:

a) Para registrar nuestros datos personales debe solicitarse un consentimiento previo, donde podamos aceptar o rechazar el registro y las consecuencias de cada una de las opciones.
b) Cuando se nos solicite el registro de datos personales, debe indicarse la finalidad para la cual serán utilizados. Vale decir, cuando aceptamos el registro de nuestros datos personales debemos conocer previamente con que finalidad se los solicita y, además, no podrán ser utilizados para un fin distinto del que consentimos.
c) Como titulares de los datos tenemos derecho a que estos datos sean veraces. Por lo tanto, podemos solicitar que se nos informe qué datos hay registrados en una base de datos, que se rectifiquen si son incorrectos o eliminados si son improcedentes. Los responsables de las bases de datos están obligados a dar cumplimiento a estos requerimientos.
d) Adicionalmente, los responsables de las bases de datos deberán establecer mecanismos adecuados para garantizar la seguridad de los datos y su reserva.

3) *¿Cuál entienden es la situación "actual" (previo a la ley) respecto al manejo base de datos que hacen las firmas? ¿Qué situaciones se dan, se comercializan sin control? ¿Cuáles son los tipos de mecanismos que utilizan actualmente para acceder a bases de datos?*

Antes de la Ley, se inscribían únicamente las Bases de Datos comerciales ante una Comisión que funcionaba dentro del Ministerio de Economía y Finanzas creada por la Ley Nº 17.838. Estas inscripciones fueron trasladadas a la Unidad Reguladora y de Control de Datos Personales que es quien actualmente posee dicha información, que se suma a la que proporcionan las empresas públicas y privadas que se están inscribiendo.
Respecto al manejo que hacen los sujetos obligados, de sus Bases de Datos, dicha información se extrae de los formularios de inscripción que son objeto de estudio por esta Unidad, así como de las denuncias formuladas por los particulares y de las eventuales medidas inspectivas que esta Unidad considere pertinente efectuar.
En la medida que estamos recibiendo inscripciones de reciente, aún no tenemos

información concreta que pueda determinar o hacer presumir la existencia de casos de comercialización de datos personales sin control, como se desprende de la pregunta.
En cuanto a los mecanismos que se utilizan actualmente para acceder a Bases de Datos, hay que diferenciar los mecanismos de los que dispone cualquier particular, de los que posee la URCDP en su ejercicio de poder de control.
En el caso del particular, persona física o jurídica, podrá presentarse directamente ante el responsable de la Base de Datos acreditando su identidad, a efectos de ejercer los derechos consagrados en la LPDP (de acceso, rectificación, modificación, supresión, etc.). Si la gestión no arrojara resultado, se le abre la posibilidad de ejercitar la acción judicial de hábeas data, conforme los arts. 37 y siguientes de la Ley.
En el caso de la URCDP tiene entre sus cometidos, el de solicitar información al responsable, y el de ejercer sus poderes inspectivos.

4) ¿Qué tipo de sanciones recibirán concretamente una vez se comience a inspeccionar? ¿Hasta cuándo tienen tiempo de registrar las bases de datos?

Las sanciones son las previstas en el artículo 35 de la Ley: apercibimiento, multa de hasta quinientas mil unidades indexadas y suspensión de la Base de Datos respectiva.
El plazo de registro y otros requisitos relativos a las Bases de Datos comerciales está previsto en el Decreto 664/008 de 22 de diciembre de 2008. Actualmente se encuentra vencido, aunque se continúan recibiendo inscripciones, sin perjuicio de las eventuales sanciones por su presentación tardía.
En cuanto a las Bases de Datos con fines no comerciales, aunque no se ha aprobado aún el decreto que reglamentará los plazos de inscripción, nada obsta que ya puedan inscribirse ante la Unidad.

5) ¿Cómo serán los procedimientos inspectivos?

Todavía no se encuentra aprobado el decreto reglamentario que regulará todo lo concerniente al procedimiento inspectivo. No obstante ello, podemos informar que La Unidad, habiendo tomado conocimiento de una posible infracción a la ley, en el ejercicio de sus potestades, tiene el cometido legal de realizar las inspecciones que estime pertinentes, conforme al artículo 34 literal D de la Ley. Para ello se requerirá resolución fundada del Consejo Ejecutivo.

6) ¿En cualquier situación un consumidor puede pedir ser retirado de la base de datos?

La respuesta es afirmativa, sin distingos que se trate de un consumidor o cualquier otro tipo de situación. La regla general en esta materia es que toda persona física o jurídica tiene derecho a solicitar la supresión de sus datos personales, incluidos en una Base de Datos, al constatarse error o falsedad o

exclusión en la información de la que es titular. (artículo 15 de la Ley)
El responsable de la Base de Datos deberá proceder a realizar la supresión en un plazo máximo de cinco días hábiles de recibida la solicitud o, en su caso, informar las razones por las que estime no corresponde. El incumplimiento de esta obligación por parte del responsable, habilitará al titular del dato a promover la acción de habeas data prevista en la Ley.
En el caso de datos personales contenidos en bases de datos con fines de publicidad, el titular puede en cualquier momento solicitar el retiro o bloqueo de sus datos de dichas bases (artículo 21 de la Ley).
En el caso de incumplimientos de obligaciones de carácter comercial o crediticia de personas físicas (Registro de Morosos) la ley prevé el registro por cinco años, con la posibilidad de prórroga por otros cinco años, si lo pide el acreedor de la obligación incumplida (artículo 22 de la Ley). Eso significa que este tipo de obligaciones no podrá registrarse por un período superior a los diez años, trascurrido el cual, el titular del dato podrá solicitar su eliminación.
Finalmente, si se trata de datos personales cuyo registro y tratamiento requirió del previo consentimiento para una posterior comunicación, este consentimiento es revocable (artículo 17 de la Ley).

7) *¿Qué tipo de consultas están recibiendo por parte de las empresas? ¿Cuáles son las mayores inquietudes que presentan?*

Las consultas realizadas a la Unidad son variadas. Una buena parte de ellas se centran en el plazo y la obligación de inscribirse que le cabe a determinada entidad, dudas respecto al llenado de formularios y tratamiento de datos sensibles. Para mayor ilustración, la URCDP ha confeccionado una lista de preguntas frecuentes que se encuentran en su página web con los siguientes links: www.protecciondedatos.gub.uy y www.datospersonales.gub.uy. Está en proceso de elaboración el "Manual de Usuario", el que una vez aprobado será publicado en el sitio web de la Unidad.

Siendo todo cuanto tenemos que informar, elévese a consideración del Consejo Ejecutivo.

Firmado por Dra. Ma. José Rodríguez Tadeo - Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 40 de 13 de julio de 2009.- Se informa sobre la adecuación del anteproyecto de decreto de creación del Sistema Integrado de Información del Área Social (SIIAS) a la Ley N° 18.331

Montevideo, 13 de julio de 2009

Informe Nº 40/2009
Expediente 2009/027
Ref. Adecuación Anteproyecto de Decreto de Creación del Sistema Integrado de Información del Área Social (SIIAS), a la Ley N° 18.331

Antecedentes

En ocasión de tener una charla informativa el 3 de julio de 2009, con la Gerente de Área Calidad y Gestión del Cambio del Ministerio de Salud Pública, Dra. Teresa Puppo sobre la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas (LPDP), de 11 de agosto de 2008 y sus incidencias respecto a la implementación de historias clínicas perinatales, se abordó el tema del Proyecto de Decreto del Sistema Integrado de Información del Área Social (SIIAS).

El 9 de julio siguiente, fue enviado vía correo electrónico, por parte de la Dra. Puppo, a solicitud de la Unidad Reguladora y de Control de Datos Personales (URCDP), copia del Anteproyecto del Decreto referido.

Ante las implicancias que este documento puede tener en materia de protección de datos personales, se pasará a analizar su contenido.

Contenido del Anteproyecto

En los Considerandos del Borrador se alude a la instauración del Sistema Integrado de Información del Área Social, en el marco de las competencias que por la Ley N° 17.866 se le atribuyen al Ministerio de Desarrollo Social.

Se hace mención a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) como Organismo impulsor del avance de la sociedad de la información y del Conocimiento y en esa línea del cometido que éste tiene en la promoción del mejor uso de las tecnologías de la información y las comunicaciones en: las personas, las empresas y el Gobierno. Se destacan los avances generados a nivel nacional en materia de protección de datos personales y su esencial régimen tuitivo; la puesta en práctica de un Certificado de Nacido Vivo de carácter electrónico; y la mayor eficacia y eficiencia en los procesos de diseño, selección y

otorgamiento de prestaciones sociales de forma moderna y transparente.

Se destaca que el SIIAS será el responsable de la gestión del sistema informático que integra información relativa a prestaciones sociales que son otorgadas a los ciudadanos del Uruguay, a través de la gestión de las diversas instituciones del área pública.

Los cometidos del SIIAS están previstos en el artículo 1° del Anteproyecto y son los siguientes:

a) Generar un sistema integrado de información interinstitucional que vincule datos de los distintos organismos, tanto de sus programas sociales, su ejecución y sus respectivos beneficiarios.

b) Contribuir a mejorar la definición de la población objetivo y la implementación de programas sociales a través de la generación, mayor sistematización y disposición de información actualizada.

c) Proporcionar a decisores, gestores, e investigadores una visión integrada de la política social y su alcance, al mismo tiempo que posibilitar la elaboración y el desarrollo de un plan estratégico de políticas sociales de alcance global.

d) Establecer los estándares necesarios para la articulación y coordinación de las diferentes instituciones que realizan políticas sociales integradas al sistema desde la perspectiva de un intercambio sistemático y permanente de información.

e) Modernizar los procesos informáticos de las diferentes dependencias para la entrada, modificación, análisis y evaluación de la información. Impulsar el empleo de la información para la mejor atención a los ciudadanos, propendiendo la puesta en marcha de los procedimientos de corrección de los datos por los responsables de su mantenimiento en cada organismo.

f) Aumentar la eficacia en la gestión de la información de programas sociales, a través de un monitoreo constante de la misma, como base para la mejora de la implementación de dichos programas.

g) Facilitar el acceso de la ciudadanía a la información.

En el artículo 2° se establece que el Sistema será de uso público permitiendo para aquellas secciones que así se determine, el acceso a los ciudadanos a la información de prestaciones sociales que brinda el Estado, incorporando los mecanismos de control previstos por la LPDP.

El artículo 3° establece que el SIIAS será administrado por un Comité de Dirección

que estará integrado con un representante de los siguientes "proveedores":

- Administración de los Servicios de Salud del Estado (ASSE)
- Banco de Previsión Social (BPS)
- Instituto del Niño y Adolescente del Uruguay (INAU)
- Ministerio de Desarrollo Social (MIDES)
- Ministerio de Salud Pública (MSP)

Los cometidos asignados al Comité, por el artículo 4° son los siguientes:

a) Conducir el desarrollo, puesta en producción y expansión del SIIAS hacia todos los efectores de políticas sociales.

b) Establecer, sin perjuicio de las orientaciones de la AGESIC, procedimientos de intercambio de información entre los organismos del área social, estableciendo niveles de disponibilidad, criterios de desempeño y seguridad requeridos, de carácter obligatorio para las instituciones que integren el SIIAS.

c) Efectuar recomendaciones al Poder Ejecutivo en materia de informatización de los servicios y sistemas de gestión de los organismos integrados al SIIAS.

d) Aportar al proceso de mejora de calidad de la información social comprendiendo todo el ciclo de producción de la misma (relevamiento, almacenamiento y uso).

Finalmente, el artículo 5° dispone que todos los organismos públicos prestarán colaboración en los aspectos necesarios para el cumplimiento de los cometidos del SIIAS.

Análisis

El Anteproyecto en cuestión pretende regular por vía de decreto un intercambio masivo de datos de personas y prestaciones entre diferentes Organismos que integran el Comité de Dirección (ASSE, BPS, INAU, MIDES y MSP). A su vez se propone que todos los Organismos públicos, es decir no ya los estrictamente involucrados, colaboren en la tarea de brindar los datos necesarios para el efectivo cumplimiento de los cometidos del Sistema.

Comunicación de Datos – Pertinencia

En primer término corresponde abocarse a la pertinencia de la introducción de este Sistema, por vía de decreto.

Si bien en el presente estamos ante un intercambio masivo de información, lo que supone la exteriorización de una verdadera "interoperabilidad", ante la ausencia de normativa que hasta el momento regule este aspecto, debemos aden-

trarnos pura y exclusivamente a las disposiciones de la LPDP.

Estamos ante una comunicación de datos, definida por el artículo 4 literal B), como *"toda revelación de datos realizada a una persona distinta del titular de los datos"*.
El régimen general de comunicación de datos se encuentra regulado en el artículo 17 que dispone que *"Los datos personales objeto de tratamiento solo podrán ser comunicados para el cumplimiento de fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo"*.

A tal previsión se le adicionan las excepciones establecidas en el artículo 9° de la LPDP.
El literal C) exceptúa del previo consentimiento al titular cuando 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 y en el caso de personas jurídicas a razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo d ella misma.
El literal B), por su parte, prevé la hipótesis de que los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. Esta última previsión (existencia de ley) tiene su fuente en la Directiva 95/46/CE, art. 11.2.

Ley N° 17.866 – Competencias del Ministerio de Desarrollo Social

Ahora bien, de acuerdo a lo establecido en la Ley N° 17.866, de 31 de marzo de 2005 que crea el Ministerio de Desarrollo Social a éste le compete entre otros: *"Diseñar, organizar y operar un sistema de información social con indicadores relevantes sobre los grupos poblacionales en situaciones de vulnerabilidad, que permita una adecuada focalización del conjunto de políticas y programas sociales nacionales", "Diseñar, organizar y administrar un sistema de identificación, selección y registro único de los núcleos familiares o individuos habilitados para acceder a los programas sociales, sujeto a criterios de objetividad, transparencia, selectividad, temporalidad, y respetando el derecho a la privacidad en los datos que así lo requieran"* (artículo 9°, literales D y E).

Es decir que si bien la implementación del sistema que se pretende es por decreto, existe una habilitación primigenia que tiene rango legal y deriva de las disposiciones transcriptas. A ello se le añade la otra excepción que establece el artículo 9° de la LPDP que contempla que los datos se recaben para el ejercicio de funciones propias de los poderes del Estado.

Parece vislumbrase de las funciones propias del Ministerio de Desarrollo So-

cial, que en el cometido de un diseño global de políticas sociales, el SIIAS pretende ser una herramienta fundamental, habida cuenta del objetivo de generar un registro único de personas donde se establezca quiénes son beneficiarios de los programas sociales que brinda el Estado y cuáles son los beneficios que reciben.

Consideración de los Principios Generales de Protección de Datos Personales

Ahora bien, que la recolección, tratamiento y/o comunicación de datos se encuentre habilitada por ley, o sea necesaria para el cumplimiento de fines del Estado, no significa que se convierta en *"res nullius"* o cosa de nadie, como lo ha destacado la Unión Europea en Dictamen 3/99 con relación a la Información del Sector Público y Protección de Datos Personales. Así, en dicho documento se estableció que el carácter público de un dato de carácter personal que resulte de una normativa o de la voluntad de la propia persona a la que alude el dato, no priva, ipso facto y para os se limiten en el caso de personas físicas a nombres y apellidos, siempre, a dicha persona de la protección que le garantiza la ley en virtud de los principios fundamentales de defensa de la identidad humana.[15]

La legislación española -artículo 21.1 de la Ley Orgánica 15/1999 (LOPD)-permite que se puedan comunicar datos personales de una Administración Pública a otra, cuando ambas Administraciones tengan competencias semejantes que versen sobre materias comunes. *"Esto es muy importante porque las competencias en materia de servicios sociales se encuentran muy repartidas entre los distintos niveles administrativos. Muchos sistemas públicos de servicios sociales se estructuran en dos niveles de asistencia, primaria y especializada, atribuyendo el primer nivel a los Ayuntamientos y el segundo a las CC.AA. La prestación de los servicios sociales solo es eficaz si las Administraciones Públicas competentes colaboran entre sí, lo que implica, en este caso, la comunicación de información personal" (…) En muchos supuestos es aplicable la previsión legal que permite la comunicación de los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra -art. 21.2 LOPD-. También es legítima la cesión de datos de los servicios sociales públicos a otras Administraciones Públicas cuando tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos -art. 11.2 e) LOPD-.*[16]

Se ha dicho con acierto en España, que los Servicios Sociales, a menudo tienen que comunicar datos especialmente protegidos, que, al igual que su tratamiento, tienen un régimen más estricto. *"Será necesario pedir un consentimiento expreso y por escrito para la comunicación de datos de ideología, religión o creencias*

15 Dictamen 3/99 relativo a Información del sector público y protección de datos personales Contribución a la consulta iniciada con el Libro Verde de la Comisión Europea titulado La información del sector público: un recurso clave para Europa, aprobado el 3 de mayo de 1999.

16 Protección de Datos Personales para Servicios Sociales Públicos, Edición Agencia de Protección de Datos de la Comunidad de Madrid, 2008O, pág. 43-44.

y un consentimiento expreso para la comunicación de datos de salud, salvo que la comunicación tenga como finalidad prestar un servicio al responsable del fichero y encaje en la figura de encargado del tratamiento. Para evitar este consentimiento expreso en algunos supuestos, es conveniente aplicar el principio de calidad, que implica comunicar los datos mínimos -posiblemente solo de contacto- y ningún dato especialmente protegido. La existencia de una previsión legal permite la comunicación de datos de raza, salud o vida sexual sin consentimiento del interesado" [17] *(...) "Por tanto, los servicios sociales solo pueden tratar datos de raza, salud o vida sexual con el consentimiento expreso del interesado o la presencia de una habilitación legal, no pudiendo admitirse la excepción del consentimiento para el cumplimiento de una función administrativo o la existencia de una relación negocial. Además, los servicios sociales solo podrán tratar datos de ideología, religión o creencias con el consentimiento expreso y por escrito del interesado y con la advertencia expresa de su derecho a no prestarlo -art. 7.1 y 2 LOPD-. Es especialmente importante en el ámbito de los datos especialmente protegidos el respeto al principio de calidad de forma que no se traten datos que no sean claramente adecuados y pertinentes para la finalidad. Así, la historia social solo podrá recoger aquellos datos que puedan afectar o repercutir en la situación personal y social del usuario de la prestación social -por ejemplo, situaciones de discapacidad física o psíquica reconocida legalmente o de hecho-".*[18]

Traspolando dichos conceptos y siguiendo la línea contextual de la LPDP concluimos que en la puesta en funcionamiento del SIIAS deben tenerse presentes los principios consagrados en la Ley, fundamentalmente los de veracidad, finalidad, seguridad y reserva.

El borrador de decreto hace referencia a:

- la misión de la AGESIC como impulsor del avance de la sociedad de la información y del conocimiento;
- los avances generados a nivel de la legislación nacional en materia de protección de datos personales que determina un régimen de protección a todos los datos personales registrados en cualquier soporte susceptible de tratamiento;
- los organismos de control previstos por la Ley N° 18.331 (Protección de Datos Personales y Acción de Habeas Data);
- establecer, sin perjuicio de las orientaciones de la AGESIC, procedimientos de intercambio de información entre los organismos del área social, estableciendo niveles de disponibilidad, criterios de desempeño y seguridad requeridos, de carácter obligatorio para las instituciones que integren el SIIAS.

No obstante, dado el flujo de información que implica el SIIAS, la informante entiende que se debería ser más explicito en la incorporación de los principios aludidos de modo expreso en el decreto, a la vez que sería necesario

17 Ob. Cit., pág. 38.

18 Ibídem, pág. 34-35

hacer una mención al tratamiento de los datos sensibles.

Por otra parte, no se ve con buenos ojos, a la luz de las disposiciones de la LPDP que el sistema sea de uso público, como prevé el artículo 2°.

Debemos diferenciar lo que es la información interinstitucional, que implica la vinculación de los datos de los distintos organismos, con el acceso que puedan tener terceros respecto a los datos que el sistema está dispuesto a incorporar. En relación a los distintos Organismos, de acuerdo a lo expuesto supra, estarían dadas las condiciones requeridas para su intercambio, habida cuenta de las disposiciones de la Ley 17.866 y el cometido concreto que posee el MIDES. Ahora bien, con relación a terceras personas, las excepciones aludidas no serían aplicables, por lo que solo podrían acceder a los datos que contempla el literal C) del artículo 9° de la LPDP o a aquellos que arrojen datos estadísticos, disociados de sus titulares.

De acuerdo a lo que surge del documento de fecha 22 de diciembre de 2008 de Resumen de Requerimientos Técnicos del SIIAS, el sistema proporcionará información en dos planos: Individual: que permita construir un "mapa" de las prestaciones y coberturas en el plano social con que cuenta cada persona, y el o los grupos que la incluyen; Estadístico: que proporcione indicadores prediseñados y referidos al área social, construidos a partir de volúmenes de datos importantes, y con referencias a la localización geográfica.

En esa línea se entiende que el acceso a la totalidad de la información tanto individual como estadística solo podrá ser entre los organismos involucrados y para la consecución de la finalidad que se pretende. Así en el caso de la Administración de los Servicios Sociales del Estado (ASSE) del MSP, sería necesario conocer el entorno psicosocial del individuo para brindarle una mejor cobertura asistencial de salud. El INAU, por su parte podría proporcionar una cobertura integral si conociera las condiciones del hogar o núcleo familiar en el que se desenvuelve el beneficiario y su desempeño en la educación pública. Y el MIDES podría relevar información sobre un conjunto de personas que les corresponde un beneficio que no están cobrando (según surge del documento).

Conclusiones

En atención a las consideraciones apuntadas, resultaría posible la implementación del SIIAS como organismo responsable de la gestión del sistema informático que integra información relativa a prestaciones sociales que son otorgadas a los ciudadanos del Uruguay, a través de la gestión de las diversas instituciones del área pública.

Si aconsejáramos un "ideal" de regulación lo haríamos en el sentido de una im-

plementación del sistema por vía legal, no obstante y atento a los fundamentos expresados supra sería legítima la introducción del mismo a través de decreto por cuanto existe una habilitación legal primigenia proveniente de la Ley N° 17.866 y además estaría en juego el "ejercicio de funciones propias de los poderes del Estado", como reclama el literal B) del artículo 9° de la LPDP en remisión del artículo 17 de la misma norma. Sobre este punto, vemos que dicho literal no establece los dos requerimientos en forma conjunta, sino que es totalmente legítima la comunicación de datos no requiriéndose el previo consentimiento informado del titular, cuando lo sea por una u otra causa, es decir, en virtud del ejercicio de funciones propias de los poderes del Estado o por una obligación legal. La conjunción disyuntiva "o" así lo indica.

En referencia a que el sistema sea de uso público caben las siguientes puntualizaciones:

Entre los Organismos involucrados existe un flujo bidireccional, en tanto aportan y consultan información. Entre estos Organismos que integran el Sistema y aquellos a los que se les solicita cooperación, el flujo de información debe ser sin trabas a los efectos de poder garantizar una mayor eficacia y eficiencia en los procesos de diseño, selección y otorgamiento de prestaciones sociales de forma moderna y transparente. No obstante deberán tener siempre presente los principios de finalidad, veracidad, seguridad y reserva consagrados en la LPDP. Así, los datos que se recojan deberán ser adecuados, ecuánimes y no excesivos en relación con la finalidad; no podrán ser utilizados para finalidades distintas o incompatibles con las que motivaron su recolección; deberán adoptarse medidas de seguridad y confidencialidad; y las personas que se dediquen a la obtención y tratamiento de los datos personales; y guardar estricto secreto profesional, so pena de incurrir en el delito consagrado en el artículo 302 del Código Penal.

Por otra parte, deberá tenerse particular atención con los datos especialmente protegidos, esto es, los datos sensibles y los relativos a la salud. De acuerdo a la definición que da el artículo 4° de la LPDP, dato sensible es aquel que revela origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual. El artículo 18 edicta que éstos solo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular o cuando medien razones de interés general autorizadas por Ley, cuando el Organismo solicitante tenga mandato legal para hacerlo, o cuando se traten con fines estadísticos o científicos, cuando se disocien de sus titulares. El artículo 19 de la LPDP, por su parte, prevé el tratamiento de los datos relativos a la salud por parte de los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud de los pacientes que acudan a los mismos o que hubieren estado bajo tratamiento de aquellos, respetándose el debido secreto profesional.

De manera que en el ejercicio de la actividad de los Organismos involucrados,

será estrictamente necesario en la recolección, tratamiento y eventual comunicación de estos datos, el consentimiento expreso del titular.

El acceso al público en general será restringido a los datos que contempla el literal C) del artículo 9° de la LPDP o a aquellos que arrojen datos estadísticos, disociados de sus titulares.
Se sugiere, en consecuencia, que el artículo 2° del Proyecto de Decreto quede redactado de la siguiente manera:

"Este Sistema permitirá el libre flujo de información entre los Organismos Públicos involucrados y aquellos de igual naturaleza que se les solicite colaboración en el marco del cumplimiento de los cometidos del SIIAS, respetándose especialmente los principios de finalidad, veracidad, reserva y seguridad consagrados en la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008.
En la recolección, tratamiento y comunicación de datos sensibles entre los Organismos involucrados, será necesario el previo consentimiento expreso del titular de los datos.

Fuera de los casos contemplados en el inciso anterior, el acceso público será reservado a los datos estadísticos o a aquellos que sin revestir ese carácter se encuentren disociados de sus titulares"

Es todo cuanto tengo que informar.

Firmado por Dra. Ma. José Rodríguez Tadeo
Derechos Ciudadanos

Informe N° 53 de 31 de julio de 2009.- Se informa sobre consulta realizada por la Junta Departamental de Maldonado sobre la publicidad de determinados datos personales en su sitio web

Montevideo, 31 de julio de 2009

Informe N° 53
Ref.: Consulta sobre la aplicación de la Ley N° 18.331 a la publicidad de determinados datos personales.

Antecedentes:

El 27 de julio de 2009 se presentó ante la Unidad Reguladora y de Control de Datos Personales (en delante URCDP) la Junta Departamental de Maldonado solicitando la opinión de la Unidad respecto a la publicidad de determinados datos personales contenidos en expedientes divulgados en su web y cómo adecuarse a la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (en adelante LPDP).

Análisis:

Primeramente se debe determinar si se está ante datos personales. A esos efectos, el artículo 4, literal d) de la LPDP los define como "*información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables*". En los expedientes remitidos por la Junta Departamental de Maldonado se encuentran datos personales como por ej. los nombres, las direcciones, los teléfonos, entre otros.

La consulta hace referencia a si es adecuado publicar en la página web de la Junta los datos personales contenidos en los expedientes que ésta lleva. Para ello se deben evaluar varios aspectos del problema planteado.

Es así, que para el tratamiento de datos personales se debe tener en cuenta el principio de finalidad recogido en el art. 8 de la LPDP, por el cual, los datos personales no deben utilizarse para una finalidad distinta o incompatible para la que fueron recabados, debiendo procederse a su eliminación cuando se haya extinguido su finalidad. Las personas denunciantes en el expediente brindaron sus datos personales para ser incluidos en expedientes de solicitudes de edificación, no surgiendo expresamente que se haya brindado el consentimiento para la publicación de sus datos en la web. Por tanto, se estaría ante un uso que va más allá de la finalidad buscada cuando se recolectaron.

Relacionado con el principio de finalidad se debe considerar la proporcionalidad en el tratamiento de datos personales. Es una muy buena práctica la publicación de toda la actuación de la Junta Departamental, que ayuda al desarrollo de la democracia y a la transparencia de la gestión, tanto es así que en España se habla de que "*Existe también una información administrativa municipal sometida al principio de publicidad. Esta publicidad está orientada a favorecer una mayor transparencia administrativa –un mayor control social de su actividad – y a facilitar la participación de los ciudadanos en los asuntos públicos* (Protección de Datos Personales en las Administraciones Locales, APCM, Pág. 59).

Aún así, es desproporcionado publicar los datos personales de los ciudadanos que acuden a la Junta a realizar una gestión de su propio interés y no tienen conocimiento de la utilización que se va a hacer de sus datos personales.

Con respecto al tratamiento de datos personales la LPDP establece como principio general la necesidad del consentimiento del titular y sus excepciones. En ese sentido, el art. 9 de la LPDP dispone la necesidad de recabar el consentimiento en forma libre, previa, expresa e informada, debiendo documentarse el mismo. Dicho artículo prevé que cuando se traten de listados cuyos datos se limiten a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento, no será necesario recabar el consentimiento del titular.

En este caso concreto, tenemos que estos datos se podrían publicar sin su previo consentimiento, pero se están publicando otros datos personales como por ej. el teléfono, que sí requieren el consentimiento expreso y previo del titular, no surgiendo éste en ninguna parte del expediente. En consecuencia, se está frente a un tratamiento excesivo de los datos personales.

Tampoco se consideran aplicables ninguna de las otras excepciones contenidas en el art. 9 de la LPDP.

Para poder superar este obstáculo podemos recurrir al procedimiento de disociación definido en el art. 4 literal G) como "*todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable*". De esta manera no se identificaría a las personas y por tanto no se requeriría el previo consentimiento del titular.

A este respecto la Agencia Vasca de Protección de Datos en su Manual de Buenas Prácticas referida a la aplicación de la protección de datos personales, establece que con las técnicas de disociación de datos se debe destruir las referencias que identifiquen al titular. Para eso se puede borrar o pintar el dato de forma que no se pueda recuperar éste de ninguna forma y, en caso de no poder hacerlo de esta forma, recurrir a la técnica del tachado.

En la situación planteada nos encontramos en una situación donde confluyen la privacidad y el acceso a la información. Para poder encontrar una solución al problema se deberá tratar de lograr el equilibrio entre ambos derechos. Por consiguiente, para lograr la publicidad de la función administrativa de los órganos estatales y mantener la privacidad de los datos personales involucrados, se ha trabajado a nivel legal y doctrinario en el concepto de "versiones públicas" de los documentos. En doctrina a esta solución se la conoce como "principio de divisibilidad", estableciéndose que se deberá dar a conocer aquellas partes o secciones que no sean clasificadas como confidenciales.

Conclusiones

Considerando los principios de finalidad y previo consentimiento informado así como todo el marco normativo existente en lo que refiere a la regulación de datos personales se entiende que no correspondería publicar *in totum* los expedientes de la Junta Departamental. Se deberían realizar versiones públicas de los documentos que se publican en su sitio web que no revelaran datos personales de los ciudadanos mediante la utilización de las técnicas de disociación de datos personales mencionados y aplicando el principio de divisibilidad de la información.

Firmado por Dra. Flavia Baladán
Derechos Ciudadanos

Informe N° 76 de 29 de setiembre de 2009.- Se informa sobre las transferencias internacionales de datos personales en el derecho comparado y su aplicación conforme la Ley N° 18.331

Montevideo, 29 de septiembre de 2009

Informe N° 76
Ref. Las transferencias internacionales de datos personales en el Derecho Comparado y su visión desde la perspectiva de la Ley Nº 18.331.

Introducción

En el marco de la sociedad de la información, las tecnologías de la información y comunicación (TIC) se convierten en un instrumento clave para el intercambio y producción de la información. En la actualidad, existe un intercambio continuo y automatizado de datos entre las empresas de todos los países, debido a las ventajas que para ello brindan las nuevas tecnologías, a los efectos de la realización de las actividades que conciernen a su giro o actividad.

Al respecto, interesa considerar aquellos aspectos que, relacionados con la protección de los datos personales, necesitan de un especial resguardo, atendiendo especialmente a aquellas situaciones donde existe un constante flujo de estos entre los distintos Estados y Organismos

En el presente informe, haremos un estudio de las transferencias internacionales en el derecho comparado, especialmente la normativa dispuesta en el ámbito de la Unión Europea.

Se hará un análisis general de los instrumentos establecidos en el ámbito de dicha comunidad, para así poder apreciar, que se entiende por transferencias internacionales, cuáles son sus características principales, quienes son sus destinatarios, entre otros aspectos relevantes.

Posteriormente, iniciaremos el estudio de la situación existente en nuestro ordenamiento positivo.

Analisis

Como mencionamos anteriormente, nos detendremos a estudiar los aspectos relacionados con las transferencias internacionales de datos personales en el ámbito de la normativa internacional existente en la materia.

A) Concepto de Transferencias Internacionales

Tanto la Directiva 95/46/CE como el Convenio Nº 108, no definen qué se entiende por transferencias o flujo transfronterizo de datos, término este, contenido en la redacción del Convenio precedentemente mencionado.

Para encontrar un concepto de estas, nos tenemos que remitir a la legislación española. Más precisamente el Real Decreto Nº 1332/94 en su artículo 1, el cual las define como *"el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de datos por correo o por cualquier otro medio convencional".* [19]

Por su parte en la Instrucción 1/2000 de la Agencia Española de Protección de Datos, relativa a las normas por las cuales se rigen los movimientos internacionales de datos de carácter personal, define a las transferencias internacionales *como "toda transmisión de datos de carácter personal fuera del territorio español".* [20]

La Sentencia dictada por el Tribunal de Justicia de las Comunidades Europeas (TJCE)[21], establece que, *"(…) cabría definir la transferencia de datos personales como la transmisión directa de datos a consecuencia de la cual el trasmitente da acceso o permite el conocimiento de ellos al destinatario (distinto del afectado), implicando por tanto una comunicación "material" de datos personales, con independencia de su finalidad".*

También encontramos un concepto de transferencias internacionales, en una de las recomendaciones dictada por la Organización para la Cooperación y el Desarrollo Económico (OCDE). Esta establece que*: "por circulación transfronteriza de datos personales se entenderá los movimientos de datos personales a través de fronteras nacionales".*

B) Tipos de Transferencias Internacionales

La Instrucción española 1/2000 de 1 de diciembre de 2000 precisa que, bajo el concepto de transferencias internacionales se incluyen aunque no de forma exhaustiva, tanto las transferencias que constituyan una cesión o comunicación de datos strictu sensu (esto es de responsable a responsable) como las que tengan por objeto la realización de un tratamiento por cuenta del responsable del fichero (esto es, de responsable a encargado)[22.]

19 El Real Decreto mencionado es reglamentario de la Ley Orgánica Española Nº 5/1992 (LORTAD). Aunque dicha Ley fue derogada por la actual LOPD, este reglamento sigue vigente en todo lo que no contradiga a esta última.

20 La Agencia Española de Protección de Datos (AEPD) tiene como función dictar instrucciones precisas para adecuar los tratamientos a los principios de la LOPD.

21 Sentencia del 6 de noviembre de 2003 Caso "Lindqvist" Nº 101/01. Disponible en www.aepd.es/sentencias, visitada con fecha 25 de septiembre de 2009.

22 ÁLVAREZ RIGAUDIAS, Cecilia "Las transferencias internacionales de datos personales y el nivel

En palabras de Lina Ornela Nuñez y Edgardo Martinez Rojas[23], *"de acuerdo al ordenamiento español, es posible distinguir dos tipos de transferencias internacionales, en función de la calificación del sujeto receptor de los datos".*

"La primer modalidad se encuentra recogida en el art. 11 de la LOPD, según la cual el sujeto trasmitente puede provocar una cesión o transmisión de datos a un tercero localizado en el extranjero, operación que supone que el tercero que actúa por cuenta propia decidiendo sobre la finalidad, uso y contenido del tratamiento. La segunda modalidad está relacionada con el art. 12 de la LOPD, ya que en esta el sujeto que comunica los datos, lleva a cabo la transmisión de los mismos, a otro sujeto ubicado en el extranjero para que se realice un determinado tratamiento a su nombre y por su cuenta".

C) Nivel adecuado de protección

Tanto la Directiva 95/46/CE (en adelante la Directiva), como el Convenio N° 108 contienen una serie de obligaciones y derechos relativos a la protección de datos personales. Al respecto de las transferencias o serie de transferencias que se realicen o prevean realizar a terceros países, son bastantes uniformes en el contenido de sus normas. Al tenor de estas, encontramos las Directrices dictadas por la OCDE y las Directrices dictadas por la ONU.

En este contexto, las normas expuestas (fundamentalmente la Directiva) contienen disposiciones concernientes a los principios aplicables a la protección de datos personales, a los medios de procedimiento para asegurar el cumplimiento de las normas, así como también disposiciones relativas a los órganos de control.

El Grupo de protección de las personas en lo que respecta al tratamiento de los datos personales, más conocido con el nombre de "Grupo del artículo 29", fue creado por el art. 29 de la Directiva. Este, posee carácter consultivo e independiente. Entre sus cometidos, se encuentra el relativo al dictado de Dictámenes sobre el nivel adecuado de protección existente dentro de la Comunidad Europea y en otros países.

Este Grupo, elaboró un documento de trabajo relativo a las transferencias de datos personales a terceros países, el cual tomaremos como referencia fundamental a los efectos del análisis del presente capitulo[24].

Para realizar un correcto estudio, acerca de que se entiende por nivel adecuado de

equiparable o adecuado de protección". Departamento de C.S.D.I de Uría Mendez (Madrid)

23 ORNELA NUÑEZ, Lina y MARTINEZ ROJAS, Edgardo "Transferencias internacionales de datos personales: su protección en el ámbito del comercio internacional y de seguridad nacional". Publicado en Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, www.juridicas.unam.mx, visitada con fecha 25 de septiembre de 2009.

24 WP 12 "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE". Disponible en http://www.edps.europa.eu/EDPSWEB/edps/lang/en/Home/Consultation/OpinionsC. Página visitada el 26 de septiembre de 2009.

protección, el Grupo del artículo 29 (en adelante G29) toma como punto de partida el análisis de dos aspectos fundamentales. Estos, serían necesarios para evaluar si el nivel ofrecido de protección es adecuado o no. Estos aspectos son, núcleo de principios de contenido de protección de datos y requisitos de procedimiento de aplicación:

1) Principio de limitación de objetivos: los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no es incompatible con el objetivo de la transferencia. Las excepciones a este principio las encontramos en la Directiva de la Unión Europea.[25]

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 pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

3) *Principio de transparencia:* debe informase 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 a lo expuesto, las encontramos en el art. 13 y 11.2 de la Directiva.

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, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

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.

6) Restricciones respecto a transferencias sucesivas a otros terceros países: únicamente debe permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país, en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el art. 26.1 de la Directiva.

Para poder evaluar el carácter adecuado de protección, el G29 afirma que es necesario distinguir los objetivos de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimientos judiciales y no judiciales utilizados en terceros países.

25 La Directiva 95/46/CE en su art. 13 prevé las limitaciones y excepciones relativas al alcance de las obligaciones y los derechos previstos en ella. Entre estas limitaciones encontramos las relativas a: la seguridad del Estado, la defensa, la seguridad pública, la prevención, investigación, la detección y la represión de infracciones penales, ente otras.

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

1) *Ofrecer un nivel satisfactorio de cumplimiento:* estos es, que los responsables conozcan muy bien sus obligaciones y los interesados conozcan muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas, disuasorias y sistemas de verificación directa por las autoridades.

2) *Ofrecer apoyo y asistencia a los interesados:* el interesado debe tener la posibilidad de hacer valer sus derechos con rapidez, eficacia y sin costes excesivos.

3) *Ofrecer vías adecuadas de recurso a quienes resulten perjudicados:* esto es, en caso de que no se observen las normas, obtener una resolución arbitral o judicial y en su caso, las indemnizaciones y sanciones correspondientes.

En resumen, se deben cumplir los preceptos enunciados en el art. 25.2 de la Directiva, es decir, cumplimientos de las obligaciones de los responsables del tratamiento, un cuerpo normativo que contemple principios básicos de protección de datos personales, medios para su eficaz ejercicio, y la existencia y control de las autoridades de protección de datos personales.

Por otra parte, nuestra normativa, sigue los lineamientos establecidos en la Directiva 95/46/CE, ya que establece como regla general, la prohibición de realizar transferencias internacionales a aquellos países que no cuenten con un nivel de protección adecuado en la materia.

Ahora bien, para comprender que se entiende por nivel adecuado de protección según nuestra Ley, no necesitamos esfuerzo alguno, ya que de hecho, el propio art. 23 de la LPDP, establece que *"(…) niveles de protección adecuados a los estándares del Derecho Internacional o Regional en la materia".* Por lo que a la hora de evaluar este aspecto, se deberá estar a lo dispuesto, por la Directiva 95/46/CE, las Decisiones de la Comisión Europea, los Dictámenes del G29 y todos los instrumentos que en su oportunidad estudiamos.

D) Excepciones

El art. 26.1 de la Directiva establece una serie de excepciones aplicables al requisito de autorización de las transferencias internacionales a terceros países. Estas, como excepción a la regla deben ser de interpretación restrictiva.

A continuación, nos detendremos en el estudio de dos de estas excepciones.

a) Q*ue el interesado haya dado su consentimiento inequívocamente a la transferencia prevista*: según la misma Directiva, el consentimiento debe ser específico, libre e informado. Por lo tanto, el interesado debe estar debidamente informado acerca de la transferencia a realizarse y el riesgo que implica el hecho

que sus datos se transfieran a otro país. Además, cualquier duda de la obtención del consentimiento se tendrá como invalidez del mismo, hecho el cual se desprende del vocablo "inequívocamente" utilizado por la norma descripta.

b) *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 o;*

c) *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.*

Al respecto, el G29 afirma que estas excepciones son potencialmente amplias, pero es posible que su aplicación práctica se vea limitada por la "prueba de necesidad": todos los datos transferidos deben ser necesarios para la ejecución del contrato. Así, si se transfieren datos complementarios que no son esenciales o si el objetivo de la transferencia no es la ejecución del contrato sino otro, como por ejemplo la mercadotecnia de seguimiento, se invalidará la excepción. Respecto de las situaciones precontractuales, solo abarca las situaciones iniciadas por el interesado, a modo de ejemplo una solicitud de información de un servicio en particular.

Los casos donde podrían aplicarse dichas excepciones, serían en las situaciones de transferencias necesarias para reservar un billete de avión de un pasajero, transacciones necesarias en el ámbito de un Banco internacional o pagos con tarjeta de crédito.[26]

E) Cláusulas contractuales tipo

Según la Directiva, la regla general es, que para que se pueda realizar una transferencia internacional, el país tercero deba contar con un nivel de protección adecuada (art.25.1). Sin embargo, y de acuerdo a lo dispuesto por el art. 26.1 del mismo cuerpo normativo, se podrá autorizar la realización de una transferencia internacional "*cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto de los respectivos derechos; dichas garantías podrán derivarse, en particular, de* ***cláusulas contractuales apropiadas".***

Como antecedentes a la práctica respectiva de las cláusulas contractuales, encontramos un estudio acerca de un modelo tipo de contrato para garantizar un nivel equivalente de protección. Dicho documento, se elaboró ante el consejo de Europa, la Cámara de Comercio Internacional y la Comisión Europea.[27]

26 Oc. Cit. WP 12

27 Model Contract to ensure equivalent data protection in the context of transborder data flows, with explanatory memorandum. Estrasburgo, 2 de noviembre de 1992.

En palabras del propio G29, en el contexto de las transferencias internacionales a terceros países, el contrato es un medio que permite al responsable del tratamiento ofrecer garantías adecuadas al trasmitir datos fuera de la Comunidad Europea a un país donde el nivel de protección no sea suficiente. Para que una cláusula contractual pueda cumplir esta función, debe compensar de manera satisfactoria la ausencia de una protección adecuada mediante la inclusión de los elementos esenciales de la misma que no existen en una situación determinada.

A los efectos de realizar el análisis de las cláusulas contractuales tipos, nos basaremos fundamentalmente en las consideraciones realizadas por el G29. Luego, nos detendremos en las Decisiones dictadas por la Comisión Europea y sus principales reflexiones.

El art. 26 de la Directiva se refiere a "garantías suficientes", para analizar el significado del mismo se debe tomar el concepto de protección adecuada y sus características, las cuales ya fueron analizadas.

Por lo tanto, el primer requisito para que una solución contractual se adapte a los requerimientos solicitados en rigor de la Directiva, es cumplir con los principios de contenido ya enunciados.

Claro, cada contrato tiene sus particularidades, por eso es preciso determinar las cláusulas relativas a la protección de los datos personales de una manera minuciosa y no solo regulando los aspectos generales que atienen a cada contrato en particular. Ese detenimiento en el análisis de cada cláusula contractual, será fundamental a los efectos de que se considere como nivel adecuado.

Al evaluar la efectividad de una solución contractual, se debe estar a ciertos criterios establecidos, los cuales ya fueron enunciados al referirse al nivel adecuado de protección.
Sin perjuicio de ello, vamos a estudiar cada uno de estos más detenidamente.

1) *Vías de recurso a disposición de los interesados:* de las consideraciones que realiza el G29 al respecto podemos decir que, el solo hecho de brindar al interesado una forma de recurso legal pertinente no es suficiente. Sería necesario, atendiendo a cada legislación en particular, estipular en el contrato celebrado entre la empresa remitente o exportadora de los datos personales derechos a los interesados titulares de los datos personales objeto de la transferencia.

2) A esto le podríamos agregar, la posibilidad de estipular el sometimiento de las partes a un árbitro internacional a los efectos de resolver cualquier cuestión que se suscitare.
   Al respecto, existen numerosos Códigos de Autorregulación sectoriales que incluyen este tipo de soluciones.
   De esta forma, el interesado se resguarda, no solo de los conflictos que pu-

dieren surgir en lo respectivo al tratamiento de los datos personales de que es titular, sino que tiene la vía abierta de poder recurrir a los mecanismos de reclamación existentes en otras materias.

3) *Apoyo y asistencia a los interesados: e*n otro orden de cosas, las cláusulas contractuales deberían incluir aquellas relativas al apoyo y asistencia de los interesados, otorgando la posibilidad de control e investigación, por parte de las autoridades de control de datos personales.
   Al respecto existen básicamente dos posibilidades de confección de las cláusulas contractuales.

En primer lugar, se puede exigir contractualmente que la autoridad de control del Estado donde estuviere establecido el remitente, pudiere inspeccionar el tratamiento realizado por el encargado del mismo en el tercer país.[28]

En segundo lugar, se puede exigir que las partes transfieran información a la autoridad de control, de cualquier tipo de quejas recibidas por parte de los interesados.
Como vemos, resulta complicado determinar si este tipo de soluciones son posibles en la práctica.

En todo caso, dependerá del tipo de legislación vigente de que se trate, y si la autoridad de control puede ser o no parte del contrato suscrito entre el remitente y receptor de los datos personales. Nosotros agregamos que, también resulta difícil la implementación de la posibilidad de inspección a empresas situadas en terceros países, atendiendo a los principios de Derecho Internacional Público existentes.

Por otro lado, en los casos de entidades bancarias o financieras, cabe la posibilidad de encontrar en las cláusulas contractuales, una salida a los efectos de poder realizar estas de una forma, si se quiere, más fehaciente. Esto es en virtud, de aquellas operaciones relativas a su giro que se realizan de forma repetitiva y similar, a modo de ejemplo, tenemos las operaciones relativas a las tarjetas de crédito. Para que las soluciones contractuales sean eficientes, se establece que cada entidad debería estar sometida a la autoridad de control de su país, en estos casos la salida contractual contaría con una mayor eficacia.

A modo de conclusión, decimos que: para evaluar la idoneidad ofrecida por una solución contractual, debe partirse de la misma base que para evaluar el nivel general de protección adecuado.

28 El art. 17.3 de la Directiva dispone: *"la realización de tratamiento por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento y que disponga en particular; que el encargado del tratamiento solo actúa siguiendo instrucciones del responsable del tratamiento".* Se desarrolla aquí el principio general de que toda persona que esté bajo autoridad del responsable debe abstenerse de procesar los datos, salvo cuando reciba instrucciones de este. De acuerdo con la Directiva un sujeto responsable del tratamiento debe asumir la responsabilidad principal del cumplimiento de los principios sustantivos de protección de datos, mientras que el sujeto encargado del tratamiento sólo es responsable de la seguridad de los datos.

Los contratos que, limitan la posibilidad de que el receptor de los datos los procese por cuenta propia de forma autónoma, ofrecen una mayor seguridad jurídica. El contrato, deberá excluir expresamente la posibilidad de que los datos sean transmitidos posteriormente a otro organismo u organizaciones no vinculados por el contrato, a menos que pueda obligárselos mediante las mismas disposiciones de protección de datos a las
que se obligan las partes.

F) Decisiones dictadas por la Comisión Europea relativas a las cláusulas contractuales tipo.

La Comisión tiene la facultad de decidir, ex artículo 26.4 de la Directiva[29], que determinadas cláusulas tipo, ofrecen suficientes garantías de conformidad con el art. 26.2 del mismo cuerpo normativo.

Existen tres Decisiones que establecen aspectos relacionados a las cláusulas contractuales tipo (en adelante CCT) que interesa señalar, estas son: la Decisión 2001/497/CE de 15 de junio de 2001 referida a las transferencias internacionales de responsable a responsable; la Decisión 2002/16/CE de 20 de febrero de 2002, referida a las transferencias internacionales de responsable a encargado del tratamiento; y la Decisión 2004/915/CE de 27 de diciembre que modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo.
En cuanto al estudio de dichas decisiones, vamos a analizar algunos puntos que nos parece interesante destacar.

De acuerdo a las dos primeras decisiones, el contrato queda sometido a las normas de protección de datos del exportador. Las CCT, responden a una estructura similar en ambos casos, previendo declaraciones y garantías de ambas partes.

Estos puntos claves a los que nos referíamos anteriormente son:

a) *Responsabilidad:* interesa señalar que, la Decisión 2002/16/CE de 20 de febrero de 2002, en el Considerando Nº 16 establece una responsabilidad solidaria, al respecto establece: *"el interesado tendrá derecho a emprender acciones, y en su caso, percibir una indemnización del exportador de datos que sea el responsable del tratamiento de los datos personales transferidos. Excepcionalmente, también tendrá derecho a emprender acción y percibir una indemnización del importador de datos en aquellos casos, surgidos del incumplimiento por el importador de datos (…)".*

29 El art. 26.4 de la Directiva establece: *"cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión".*

En cambio la Decisión 2004/915/CE de 27 de diciembre de 2004, contiene una alternativa a la responsabilidad solidaria prevista en la Decisión mencionada anteriormente. Aquella establece, un régimen de responsabilidad basado en la obligación de diligencia debida, en virtud de la cual el exportador y el importador de datos responderían ante los interesados por el incumplimiento de sus obligaciones contractuales respectivas.

El exportador, es así mismo responsable sino realiza esfuerzos razonables para determinar, si el importador es capaz de cumplir las obligaciones jurídicas que le incumben en virtud de las cláusulas pactadas (culpa in eligendo). Por lo tanto, el interesado puede emprender acciones contra el exportador de datos a este respecto. Además, esta Decisión prevé la posibilidad de realizar por parte del exportador, auditorías en las instalaciones del importador o exigirle pruebas que demuestren que dispone de suficientes recursos financieros para cumplir sus responsabilidades.

b) *Obligaciones de las partes:* tanto la Decisión 2001/497/CE de 15 de junio de 2001 como la 2002/16/CE de 20 de febrero de 2002, establecen que: *"el importador de datos tratará los datos personales transferidos sólo en nombre del exportador de datos y de conformidad con las instrucciones que reciba (…)".*

Obligaciones del exportador: las tres decisiones establecen un capitulo donde redactan de forma exhaustiva las obligaciones de las partes. Nuestra intención es simplemente recoger alguna de ellas contenidas en la Decisión 2004/915/CE de 27 de diciembre de 2004, debido a su mayor proximidad en el tiempo.

El *exportador de datos* se obliga a:

- realizar esfuerzos razonables para determinar si el importador de datos, es capaz de cumplir las obligaciones jurídicas que le incumben en virtud de las presentes cláusulas.
- responderá en un tiempo razonable, a las consultas de los interesados y de la autoridad, relativas al tratamiento de datos personales por parte del importador de datos.

El *importador de datos* acuerda y garantiza lo siguiente:

- poner en práctica las medidas técnicas y organizativas que resulten necesarias para proteger los datos personales contra, su destrucción accidental o ilícita, su pérdida o alteración accidental o su divulgación o acceso no autorizados.
- tratará los datos personales para los fines objeto de la transferencia y tiene autoridad legal para ofrecer garantías y cumplir los compromisos previstos en las cláusulas.

c) *Resolución de conflictos:* en caso de conflicto o de reclamación interpuesta con-

tra una o ambas partes por un interesado o por la autoridad de control, la una informará a la otra sobre esta circunstancia y ambas cooperarán con el objeto de alcanzar una solución amistosa lo antes posible. Las partes acuerdan así mismo, estudiar la posibilidad de participar en cualquier otro mecanismo de arbitraje, mediación u otra índole y acatar cualquier decisión de los tribunales competentes o de la autoridad del país de establecimiento del exportador de datos, cuyas decisiones sean finales y contra las que no pueda entablarse recurso alguno.

d) *Resolución de las cláusulas:* en caso que el importador de los datos incumpla, el exportador de datos podrá, suspender temporalmente la transferencia de datos personales, por ejemplo: cuando exista decisión definitiva acerca del incumplimiento de cualquiera de las cláusulas descriptas en la Decisión.

Cualquiera de las partes podrá resolver las presentes cláusulas, si la Comisión hace constar que el país al cual se transfiere los datos y en el que son tratados por el importador, garantiza un nivel de protección adecuado.

Las partes se comprometen a no modificar las presentes cláusulas y podrán introducir, anexos adicionales de forma que abarque múltiples transferencias, las cuales presentaran a la autoridad siempre que esta así lo solicite.

De acuerdo al análisis efectuado, corresponde aclarar la distinta función que cumplen los contratos según los sujetos que intervengan en ellos; en el caso de los países integrantes de la UE, el contrato es el mecanismo utilizado para definir y regular el reparto de responsabilidades en materia de protección de datos, cuando en el tratamiento interviene más de una entidad.

Sin embargo, cuando se trata de transferencias de datos a terceros países, el contrato no solo tiene la finalidad descripta anteriormente, sino que debe incluir garantías adicionales para los interesados, por el hecho de que el receptor del país no comunitario no está sujeto a una serie de normas obligatorias de protección de datos que proporcionan garantías adecuadas.

Por último, resulta relevante destacar que, este conjunto de CCT es una de las alternativas previstas en el art. 26 de la Directiva, dicha afirmación se deriva del vocablo "podrán" utilizado por la norma descripta. Ahora bien, como así lo señala la Decisión 2004/915/CE de 27 de diciembre de 2004, estos conjuntos de cláusulas contractuales existentes en las Decisiones enunciadas comprenden un todo jurídico coherente. Por lo tanto, el exportador e importador de datos personales, podrían optar por cualquiera de los conjuntos de CCT o elegir otro fundamento jurídico para las transferencias de datos. Sin embargo, cuando opten por uno de estos conjuntos, no es recomendable reconocerles la posibilidad de modificarlos total o parcialmente ni de combinarlos.

G) Las Reglas Corporativas Vinculantes

En el año 2003, el G29 publicó un documento de trabajo, sobre reglas corporativas vinculantes (RCV) para transferencias internacionales. Según la opinión de este grupo, estas reglas, en tanto estuvieran acorde a los principios de contenido identificados en el documento de trabajo sobre nivel adecuado de protección (WP 12), no habría razón para no considerarlas y por lo tanto las autoridades de protección de datos podrían autorizar transferencias multinacionales dentro de un grupo de compañías. Aquí vemos, que el ámbito de aplicación de estas reglas, se circunscribe a las situaciones de empresas contenidas dentro de un mismo grupo.

Las Reglas Corporativas Vinculantes (RCV), constituyen un instrumento adicional a las Decisiones de la Comisión Europea, que establecen requisitos adicionales para transferencias a países que no cuenten con un nivel de protección adecuado en la materia. Estas reglas, están referidas a transferencias realizadas dentro de un grupo de compañías.

Podemos decir que las RCV son códigos de conducta que contienen específicamente normas destinadas a facilitar la realización de transferencias internacionales dentro de un grupo de empresas.

Entre los requisitos que deben poseer estos mecanismos, tenemos la exigencia de obligatoriedad interna dentro del grupo y fuera del mismo.

Al igual que en las CCT, en las RCV es fundamental la aplicación del principio de cooperación internacional y la intervención de las autoridades de control en virtud de las diferencias que los regímenes de protección de datos poseen.

Cabe destacar las que referidas a la creación de un sistema de gestión de las reclamaciones de los afectados, con expresa identificación de un departamento específico a esos efectos; y la que establece la aceptación de que los interesados. pueden interponer acciones contra el grupo así como también elegir la jurisdicción competente.

El Grupo 29, también propone la adopción de reglas de procedimiento que permitan a las compañías seguir un único proceso de legitimación ante la autoridad de protección de datos de un Estado miembro, que gestionará el otorgamiento de autorizaciones con las distintas autoridades de los Estados miembros donde el grupo opera.

H) Procedimiento de Autorización de las Transferencias Internacionales

El art. 5 de la Directiva, contempla un procedimiento en que la evaluación de las transferencias se efectúa en relación con transferencias particulares o con ca-

tegorías de estas. Por lo tanto, resultaría inviable el estudio detallado de cada transferencia en particular, debido a la gran cantidad de estas que se realizan a diario por muchas empresas alrededor del mundo.

Además, existen otras complicaciones derivadas de aquellas situaciones donde, los terceros países carecen de una protección uniforme en todos los sectores económicos, o su legislación relativa a la protección de datos, se circunscribe solamente al ámbito público.

Por lo tanto, es necesario idear mecanismos que racionalicen el proceso decisorio para un elevado número de casos, permitiendo tomar decisiones o al menos decisiones provisionales, sin una demora injustificada o sin implicar recursos excesivos.[30]

Con el motivo de estudiar los procedimientos de autorización, haremos referencia al procedimiento establecido en el Real Decreto español N° 1720/2007, ya que los demás instrumentos internacionales no contienen (al menos de una forma detallada) un procedimiento a seguir en estos casos. Luego, haremos una referencia general del procedimiento que lleva a cabo la Dirección Nacional de Protección de Datos Personales (DNPDP).

Procedimiento de autorización de transferencias internacionales en el Real Decreto español N° 1720/2007.

Para comenzar decimos que, para que proceda dicho procedimiento se debe estar ante la presencia de dos cuestiones preliminares:

- que el país tercero no posea un nivel adecuado de protección declarado por la Comisión Europea; y
- que la situación no se encuentre comprendida dentro de las excepciones contenidas en el art. 34 de la LOPD.

Sin la intención de realizar un examen exhaustivo de este procedimiento, procederemos a enunciar algunas características que merecen destacarse.

- la solicitud de transferencia se hará siempre a pedido del exportador de los datos, donde deberá indicar:
- la identificación del o los ficheros de los cuales se pretende realizar la transferencia
- la identificación del código de inscripción de registro del fichero
- indicar la finalidad por la cual se pretenden realizar, y la documentación que incorpore las garantías exigibles para la obtención de la autorización.

30 Ob. Cit WP 12.

En caso de que la transferencia se fundamente en un contrato, presentación de copia de éste.

Esto es, sin perjuicio de los requisitos legales exigidos para las transferencias.
Las garantías adecuadas de los contratos presentados, atenderán el cumplimiento de las Decisiones dictadas en el ámbito de la Comisión Europea, las que ya tuvimos la oportunidad de analizar anteriormente.

Cabe agregar que, por el art. 69 del Decreto mencionado, la AEPD tiene la potestad de suspender temporalmente la realización de transferencias internacionales a un tercer Estado que ofrezca un nivel adecuado de protección, en ciertos casos enumerados, entre los cuales se encuentra, cuando la autoridad de protección de datos del país del importador u otra autoridad competente en caso de no existir las primeras, resuelvan que ha existido vulneración por parte del importador, de las disposiciones de protección de datos establecidas en su derecho interno. La suspensión se acordará previo procedimiento, el cual es similar al establecido para la solicitud de autorización de las transferencias.

Otras cuestiones relacionadas con normas de procedimiento, son las establecidas en la Norma N°III de la Instrucción española Nº 1/2000 de 1 de diciembre de 2000. Esta dispone que, la AEPD puede solicitar al responsable la documentación acreditativa de la concurrencia de cualquiera de las excepciones al principio general de recabar autorización previa, y la información relativa al cumplimiento del deber de información del interesado quién será el destinatario de los datos, así como de la finalidad que justifique la transferencia y el uso de los datos que podrá hacer el destinatario (art. 27 de la LOPD).

Procedimiento de autorización de transferencias internacionales en el ordenamiento positivo argentino:

La Ley Nº 25.326 en su art. 12.1 y el art. 12 del Decreto que reglamenta dicha Ley, regulan las transferencias internacionales de datos.

En general, las disposiciones mencionadas, siguen las líneas internacionales, fundamentalmente la correspondiente a la Directiva 95/46/CE, a la LOPD y su Decreto reglamentario. Sin embargo, a diferencia del régimen español, la normativa argentina, no contiene disposiciones expresas al respecto del procedimiento que se debe seguir para autorizar una transferencia internacional.

Cabe resaltar, la disposición que otorga la facultad a la Dirección Nacional de Protección de Datos Personales (en adelante DNPDP), a evaluar, de oficio o a petición de parte el nivel de protección brindado por las normas de un Estado u Organismo internacional.
Al respecto, y del estudio de los distintos Dictámenes que la DNPDP ha dictado, propondremos un resumen, a nuestro criterio, del procedimiento que

sigue dicha Dirección, a los efectos de la autorización de transferencias internacionales.

Procedimiento:

Antes de enumerar las distintas etapas del mismo, debemos considerar que la DNPDP siguiendo la misma línea establecida por la Directiva, establece que cuando se pretenda realizar una transferencia internacional a un Estado que no posea un nivel adecuado de protección, se deberán seguir los parámetros establecidos en el art. 25.2 y 26.2 de la misma. Esto es, que el Estado proporciona un nivel adecuado de protección, cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de los datos personales.

A) se analiza, si el país contiene un ordenamiento positivo o legislación específica sobre protección de datos personales o si posee sistemas de autorregulación, en caso negativo la licitud de la transparencia internacional, queda sometida al amparo que establezcan las cláusulas contractuales pactadas entre el exportador e importador de datos personales.

B) se recibe solicitud presentada por el exportador de datos, acompañada de copia del contrato y del formulario correspondiente. [13]

C) la DNPDP procede al estudio de cada cláusula labrada en el contrato y emite un juicio correspondiente a cada una de ellas.

D) a los efectos de evaluar dichas cláusulas, se toman como basamentos, las Decisiones dictadas por la Comisión Europea, atendiendo fundamentalmente los que, determinan que la legislación aplicable al contrato debe ser la correspondiente a la del territorio del exportador de datos (Ley Argentina); medidas de seguridad necesarias; compromiso solidario para responder en casos de incumplimientos a la Ley N° 25.326; acuerdo sobre la jurisdicción que corresponde a los efectos de la resolución de las controversias derivadas del tratamiento de los datos personales, entre otras.

E) la DNPDP, dictamina si el contrato presentado incorpora en su redacción de manera razonable y adecuada los requisitos mínimos exigibles para una transferencia de datos personales, que no son más que los ya estudiados cuando hicimos referencia a la normativa internacional relativa a las cláusulas contractuales tipo.

Por último y a modo de resumen aclarar que, a la hora de evaluar si un Estado posee un nivel adecuado de protección, tanto el derecho español como el argentino se basan en la Directiva 95/46/CE, en particular atienden a las siguientes circunstancias:

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

También analizan, el ordenamiento positivo vigente en el estado destinatario, si posee sistemas de autorregulación y el amparo que establezcan las cláusulas contractuales celebradas.

SITUACIÓN DE NUESTRO ORDENAMIENTO POSITIVO

El art. 23 de la Ley Nº 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (en adelante LPDP) establece: *"se 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".*

Luego de haber realizado un análisis de las transferencias internacionales en el derecho comparado, nos atiende ahora estudiarlas desde la perspectiva de la LPDP. Atento a ello, consideramos concentrarnos en tres aspectos fundamentales:

A) Concepto y tipos de transferencias internacionales.

Para comenzar decimos que, la LPDP no brinda un concepto de transferencias internacionales. Este, es definido por el Decreto reglamentario de dicha Ley, el que en su art. 4 literal H) dispone: "*tratamientos de datos que supone una transmisión de éstos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo".*

A juicio del informante, y con respecto a los tipos de transferencias que existen, esta definición parecería incluir, aquellas transferencias que se realicen de responsable de la base de datos al encargado del tratamiento, y aquellas realizadas de responsable a responsable de la base de datos. Esta interpretación, se estaría desprendiendo de la definición relativa a las transferencias internacionales enunciada, cuando habla de que el tratamiento se realiza por cuenta del responsable. Además, de la propia definición de importador de datos dada por el Decreto N° 414/009 de 31 de agosto de 2009, en su art. 4 literal F), se desprende que este sujeto puede ser responsable o encargado del tratamiento.

Cabe agregar a título informativo, que en el ordenamiento español se admite la figura del subencargado de tratamiento siempre y cuando se den ciertas condiciones.[14].

Es interesante destacar, cuál es el criterio para diferenciar cuando la transferencia se realiza de responsable a responsable o de responsable a encargado de tratamiento.

Cuando estamos en presencia del primer supuesto -transferencia de responsable a responsable- el receptor de los datos -importador- realiza un posterior tratamiento sobre los mismos decidiendo sober su uso, finalidad y contenido. En estos casos existe una comunicación de datos propiamente dicha, ya que el responsable cede los datos para que otro responsable realice un nuevo tratamiento sobre ellos, teniendo poder de decisión.

Por lo tanto, si es una comunicación de datos e independientemente de la circunstancia de que el país sea adecuado o no- se deberá dar cumplimiento a lo establecido en el art. 17 de la LPDP. Esto es, se deberá recabar previamente el consentimiento de los titulares, informar acerca de la finalidad de las transferencias y proporcionar información acerca de la identificación del destinatario. Asimismo, la comunicación deberá ser sólo para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y destinatario. [15]

Sin embargo, cuando estamos ante la segunda hipótesis -de responsable a encargado de tratamiento- no estamos en presencia de una comunicación de datos propiamente dicha.

Es decir, en este tipo de transferencias, el encargado de tratamiento trata los datos en virtud de las directivas recibidas del responsable o sea por cuenta ajena. En estos casos, el encargado accede a la base de datos perteneciente al Responsable, a efectos de prestar un servicio en particular, por lo que no decide sobre su uso finalidad y contenido.

B) Procedimiento de autorización de transferencias internacionales

Introducción

El inciso 2 del art. 23 de la LPDP establece: *"sin perjuicio de lo dispuesto en el primer inciso de este artículo, la URCDP 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 de tratamiento ofrezca garantías suficientes respecto a la protección a 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".*

Antes de comenzar con consideraciones específicas referidas al procedimiento, es importante destacar que, Uruguay se encuentra en trámite de adecuación de sus normas relativas a la protección de datos personales ante la Unión Europea.

La URCDP, con motivo de pronunciarse acerca de qué países cuentan con un nivel de protección adecuado, dispuso por Resolución Nº 17 de 12 de junio de 2009, seguir los lineamientos establecidos en la Directiva 95/46/CE. Atento a lo expuesto, dispuso en el Considerando IV de aquella que:"*se consideran países apropiados para las transferencias internacionales, aquellos que a juicio de la Unidad cuenten con normas de protección de datos adecuadas y medios para asegurar su aplicación eficaz".*

En esta línea de análisis, el inciso 2 del artículo 23 de la LPDP, está en concordancia con la redacción dada por el art. 26.2 de la Directiva 95/46/CE.

Atento a ello, y a que la presente Directiva y los instrumentos internacionales mencionados, son los de mayor recibo en la materia, entendemos procedente realizar una interpretación de nuestra normativa, siguiendo los criterios establecidos por aquellos. Apuntando así, a un régimen tuitivo de datos personales que se oriente a proteger eficazmente los derechos de los titulares de los datos.

Al respecto interesa destacar los siguientes puntos:

A) Legislación aplicable y Tribunal competente: este aspecto reviste de sumo interés por la doctrina internacional. Al respecto, Juan Antonio Pavón Perez afirma que: *"la especial volatibilidad de las transferencias de datos complica extraordinariamente la definición del derecho aplicable, en lo que algunos autores han calificado acertadamente como una desterritorialización cualificada. Las características de los flujos de información y el carácter abierto de las redes, hacen que los datos puedan ser accedidos, recopilados y tratados desde varias países de manera simultánea, por lo que distintos Estados tendrían competencia normativa para definir los términos y condiciones de las prácticas apropiadas en el ámbito de la información".*[16]

En oportunidad de analizar los instrumentos internacionales, hicimos referencia a que en el ámbito internacional existe una tendencia concreta, a aplicar la Ley vigente de protección de datos personales del país del exportador de los datos, en los casos que se trate de transferencias de responsable a encargado del tratamiento de estos. Este criterio, se deviene del entendido de que el país del exportador de los datos se encuentra dentro del ámbito de la Unión Europea u obtuvo un pronunciamiento favorable de la Comisión Europea al respecto del nivel adecuado de protección. Este criterio, permite brindar mayores garantías a la realización de transferencias, ya que la Ley de ese Estado contiene los principios de contenido y mecanismos efectivos para su aplicación, establecidos y recomendados por los instrumentos internacionales y los expertos en la materia.

Con respecto al Tribunal competente, interesa señalar que, la solución más acertada parece ser la existencia de un compromiso (sea contractual o no) entre el importador y el exportador de los datos, de someter cualquier tipo de conflicto que surja a una solución arbitral.

Tampoco debería dejarse de tener en cuenta, las soluciones coincidentes con la normativa de mayor recibo existente en el Derecho Internacional.

B) Autoridad de control: con el motivo de favorecer a un régimen adecuado de protección en salvaguarda de los derechos de los titulares, resulta relevante la actuación activa de las autoridades de control de protección de datos existentes en los Estados partes de la transferencia. Estas, deberían proceder de acuerdo al deber de cooperación internacional.

En el caso que uno de los Estados no tenga establecida una autoridad de protección de datos, se deberá estar sujeto a la autoridad u organismo competente en la materia.

C) Responsabilidad: la LPDP, en sede de derechos referentes a la comunicación de datos, (art. 17) dispone: "*el destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate".*

En los casos donde se presente copia del contrato, con el motivo de obtener la autorización de la URCDP, habría que analizar si las cláusulas relativas al reparto de responsabilidades son suficientes. En este caso, se podría estar a lo establecido en el art. 17 de la LPDP si así se concibiera, a las transferencias internacionales como sub tipo de cesión o comunicación de datos (art. 4 Literal H) Decreto 414/009).

D) Plazo de duración de la transferencia internacional: del análisis de los instrumentos internacionales mencionados, no se hace referencia a si es necesario que la transferencia cumpla con un plazo determinado.

De acuerdo a lo expuesto y realizando una interpretación armónica de nuestra normativa relacionada a la protección de datos personales, entendemos que el plazo razonable se debe encontrar en las disposiciones relativas, al derecho de supresión de los datos personales, al principio de finalidad, y la conservación de los datos objeto de tratamiento.

En los casos donde el titular ejerza el derecho a que se eliminen sus datos personales, la transferencia internacional debería dejar de realizarse, sólo para el sujeto que haya efectuado el ejercicio de dicho derecho.

Según el principio de finalidad (art. 8 LPDP), los datos deben ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados. Que el plazo de terminación de la transferencia sea determinado atendiendo al principio de finalidad, implica que una vez culminada la finalidad del contrato, por ejemplo, la prestación de servicios objeto de aquel, la transferencia tendría como plazo final ese hecho.

Otro elemento a tener en cuenta es que, si la transferencia de datos personales refiere en particular a los datos contenidos en una base de datos, donde exista un plazo determinado de conservación, se debería atender a este a los efectos del cómputo del plazo final de la transferencia.

Procedimiento:

Antes de comenzar decimos que, la redacción de la parte final del inciso 2 del art. 23 de la LPDP, permite que la URCDP pueda autorizar una o varias transferencias internacionales, mediante la existencia de cláusulas contractuales apropiadas u otro mecanismo que ofrezca iguales o mayores garantías. Dicha interpretación, se desprende del vocablo
"podrá" utilizado por la norma descripta.

Con el motivo de implantar un procedimiento de autorización de transferencias internacionales a seguir por la URCDP sugerimos que, para poder iniciar el procedimiento de autorización, el exportador de datos personales deberá:

A) Cumplir con el procedimiento previsto para la inscripción de la o las Bases de Datos que posea la empresa y obtener una resolución favorable de inscripción dictada por el Consejo Ejecutivo de la URCDP.

B) Realizar la solicitud de autorización de las transferencias de acuerdo al art. 35 del Decreto 414/009, la que deberá poseer el siguiente contenido:

   a. identificación de la base de datos y su código de inscripción.
   b. realización de una descripción de la transferencia, en donde se podrá informar las características generales de esta.

También, deberá indicar la finalidad que la justifica, adjuntando la documentación acreditante que entendiera correspondiente. Creemos, que dentro de la descripción que el exportador realice, sería de buena práctica recomendar que se establezca un plazo razonable por el cual se pretendan realizar las transferencias.

C) Se ingresará y formará expediente en el cual recaerá informe. En este, se controlará la documentación presentada en arreglo a las disposiciones mencionadas ut supra y se aconsejará o no la autorización.

En el caso de presentarse copia del contrato entre el importador y exportador de datos, además de proceder al control de la representación legal acreditada, se hará el análisis de las cláusulas contenidas en este, teniendo en cuenta las prácticas internacionales ya enunciadas. Esto es, siguiendo los parámetros que se enuncian en la Directiva 95/46/CE y en las Decisiones dictadas por la Comisión Europea las que son seguidos por la normativa española y argentina.

D) En el caso de verificarse observaciones se le dará vista al interesado, el que deberá evacuarlas en el plazo de 10 días hábiles.

E) Una vez levantadas las observaciones o en caso de no constatarse la existencia de estas, se elevará al Consejo Ejecutivo de la URCDP el que, atendiendo a las circunstancias del caso y tomando en cuenta los parámetros internacionales enunciados en el numeral anterior, resolverá acerca de si autoriza o no la realización de las transferencias planteadas.

En caso de recaer resolución favorable, se inscribirá la autorización de las transferencias solicitadas en el registro que a tal efecto lleva la URCDP. Esto es, en virtud del literal D) del art. 15 del Decreto 414/009.

F) Finalmente, se notificará de la resolución al exportador de datos personales y posteriormente se publicará.

A modo de sugerencia, sería interesante pensar en la posibilidad de elaborar un formulario, puesto a disposición de los interesados, donde constaran aquellos requisitos mínimos que debería cumplir la transferencia internacional. Además de los ya enunciados, estarían los datos relacionados con las empresas involucradas en la transferencia (razón social, nombre, número de RUT, ramo o actividad, entre otros). Este documento, se presentaría conjuntamente con la documentación acreditante y copia del contrato en su caso.

No obstante lo mencionado, es preciso recordar que la URCDP tiene la facultad de solicitar información a las entidades públicas y privadas, las que deberán brindar documentos relativos al tratamiento de datos personales (art. 34 literal E) de la LPDP).
Creemos que el uso de esta facultad, podría ser de buena práctica, tanto de forma previa a la autorización como durante el desarrollo de estas.

En último lugar, cabe recordar que la parte in fine del art. 35 del Decreto N° 414/009, establece que, para los casos de transferencias de empresas multinacionales, estas empresas deberán poseer códigos de conducta debidamente inscriptos ante la URCDP. La inscripción de los códigos de conducta, se regirá por el mismo procedimiento establecido para las bases de datos (art. 36 del Decreto 414/009).

C) Excepciones a la solicitud de autorización.

El mismo art. 23 de la LPDP establece, una serie de excepciones a la regla general de prohibición de transferencias internacionales, a países que no cuenten con un nivel adecuado. Sin la intención de analizar en profundidad dichas excepciones, nos detendremos en la excepción que consideramos más relevante a los efectos del presente informe.

El literal A) del art. en análisis dispone: *"que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista"*: El carácter de inequívoco significa, que no haya lugar a dudas que se ha brindado el consentimiento para realizar la transferencia, en caso de existir estas, ese consentimiento no será válido.

Este carácter del consentimiento mencionado, debería ser sumado a los caracteres establecidos en el art. 9 de la LPDP. Estos son: que sea libre (sin ser objeto de coacción alguna), previo (a la transferencia prevista), expreso (específico para esa situación) e informado, esto es que el titular de los datos personales conozca la finalidad para la cual sus datos serán transferidos.

Atento a lo mencionado, corresponde realizar algunas consideraciones que entendemos pertinentes.

En la actualidad, existen gran variedad de empresas que realizan o pretenden realizar este tipo de transferencias. A estos efectos, una de las soluciones sería, la de instrumentar un mecanismo por el cual estas recabaran y documentaran el consentimiento de los titulares, de forma previa a la realización de las transferencias internacionales.

En principio, parecería una solución de difícil implementación práctica, debido no solo a la cantidad de clientes que poseen las empresas, sino también al número de transferencias internacionales que estas realizan a diario.

No obstante lo expuesto, en los casos de transferencias relativas a operaciones de crédito y, siguiendo la tendencia internacional al respecto, podría recabarse el consentimiento previamente a la realización de estas sin necesidad de solicitarlo en cada oportunidad que se pretendan transfieran los datos con destino internacional.

A estos efectos, se deberá informar la finalidad de la transferencia, y la identidad de los destinatarios tal como lo dispone el art. 17 de la LPDP, incluso podría informarse acerca de las consecuencias que tiene que sus datos seas transferidos -siempre que estamos ante transferencias de Responsable a Responsable del tratamiento-.

Si bien esta opinión la entendemos discutible, habrá que estar a cada situación particular. Se entiende que, en los casos relativos a operaciones de crédito, las cuales se caracterizan por ser de tipo repetitivas y similares, recolectar de forma previa el consentimiento, podría llegar a excepcionar a las empresas que así lo compro-

baren debidamente, de la autorización que la Unidad Reguladora y de Control de Datos Personales (URCDP) concede a estos efectos.

Por otra parte y de acuerdo a la definición que mencionamos de transferencias internacionales, estas constituyen una cesión o comunicación de datos. Según el art. 4 literal B) de la LPDP, se dispone que, por comunicación de datos se entiende: *"toda revelación de datos personales realizada a una persona distinta del titular de los datos".*

El art. 17 de la LPDP, establece que en los casos de comunicación de datos personales, además de solicitar el previo consentimiento informado del titular, se deberá identificar al destinatario de los datos. Y agrega*: "el destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate".*

Armonizando los arts. 17 y 23 de la LPDP y el art. 4 Literal H) del Decreto reglamentario N° 414/009 de 31 de agosto de 2009, podríamos sostener que, en casos de transferencias internacionales de datos personales, los sujetos partes de la transferencia, o sea el exportador e importador de datos, fueran solidaria y conjuntamente responsables, frente a la URCDP y al titular de los datos, por el incumplimiento de las observancias legales y reglamentarias relativas a la protección de los datos personales.

Creemos que esta solución (la cual podrá ser objeto de un estudio pormenorizado) va en línea con los principios establecidos en la LPDP y apunta a proteger a los titulares de los datos personales, pudiendo estos ejercer las acciones que así lo entendieren pertinentes de una forma más efectiva.

Conclusiones

I) Las transferencias internacionales, se encuentran reguladas en distintos instrumentos normativos internacionales, y cuentan con un basto desarrollo doctrinario.

Al respecto, existe una tendencia concreta, que considera que esta temática es de tipo complejo y de naturaleza transversal.

Atento a lo expuesto, agregamos que, la naturaleza transversal de dichas transferencias puede ser visto desde dos ángulos. Por un lado, la temática desarrollada en el presente informe, no solo se encuentra relacionada a diversos aspectos regulados por otros cuerpos normativos, sino que también roza prácticamente, todos los aspectos relativos a la legislación de protección de datos personales.

II) En concordancia con la doctrina internacional imperante en la materia, sería de buen recibo el análisis de nuevas vías de mecanismos apropiados para alcanzar

un nivel adecuado de protección, que ofrezcan iguales o mayores garantías que los ya existentes. Estas nuevas vías, deberían apuntar a lograr una mayor flexibilidad y simplificación de los cláusulas contractuales y los trámites del procedimiento de autorización.

III) Con el motivo de realizar transferencias a Estados u Organismos que no cuentan con un nivel adecuado de protección, las cláusulas contractuales tipo, a pesar de su carácter voluntario, aparecen como la práctica más generalizada en pro de alcanzar la debida autorización.

IV) Creemos que, la LPDP cuenta con un rico marco normativo que contempla numerosos principios de contenido y mecanismos de aplicación, recomendados por los expertos en la materia.

V) En los casos, donde el Estado u Organismo no cuente con un nivel adecuado de protección, se deberá analizar si se ofrecen las garantías suficientes.

A la hora de evaluar dichas garantías, se deberían tomar los parámetros internacionales de mayor recibo en la materia, así como también las experiencias y prácticas recabadas por las agencias de protección de datos internacionales.

VI) En los casos donde no sean de aplicación, algunas de las excepciones contenidas en el art. 23 de la LPDP y la transferencia se pretenda realizar a un Estado sin un nivel de protección adecuado en la materia, la URCDP deberá contar con un procedimiento apropiado a los efectos de autorizar dicha situación. A la luz de lo expuesto, estamos en presencia de procedimientos complejos, que deberían ser revisados continuamente, debido a la gran variedad de situaciones que se puedan presentar en la práctica.

VII) Sin perjuicio de continuar con el estudio de la temática en análisis, el procedimiento de autorización, debería tener como meta a lograr, un adecuado balance entre los legítimos intereses empresariales, que se puedan ver perjudicados por la demora en la tramitación de la autorización y el resguardo de los derechos de los titulares de los datos personales contenidos en la normativa nacional vigente.

Firmado por Dr. Federico Carnikian
Derechos Ciudadanos

Informe N° 80 de 11 de setiembre de 2009.- Se informa sobre la incorporación de datos biométricos a la cédula de identidad y al pasaporte común

Montevideo, 11 de setiembre de 2009

Informe Nº 80/2009
Exp. Nº 2009/025: Incorporación de datos biométricos a la cédula de identidad y al pasaporte común

- I -

La *Biometría* es la ciencia que estudia la identificación de individuos a partir de un rasgo anatómico o una característica del comportamiento. En base a la aplicación de técnicas derivadas de esta ciencia, se llega a los denominados *datos biométricos*, definidos como "propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican cierto grado de probabilidad".[31]

Actualmente, y de acuerdo al estado de la técnica, existen los siguientes tipos de sistemas biométricos: [32]

a) Verificación de escritura manuscrita o firma: se basa en aspectos dinámicos (presión del lápiz sobre el papel, ángulo de los trazos, tiempo utilizado para firmar).

b) Verificación de huellas dactilares: tradicionalmente reconocida como uno de los mejores patrones identificatorios, ya que no está probado científicamente que no hay dos iguales; se basa en la lectura de la huella individual y su comparación con las existentes en el banco de datos.

c) Verificación de patrones de la mano: comparación de la imagen tomada con patrones almacenados, a través de modelos matemáticos.

d) Verificación de la voz: requiere de sala especial, ajena a ruidos y con buena acústica. El usuario se autentifica a través de un texto pre definido o independiente.

---

31 Dictamen 4/2007 sobre el concepto de datos personales, de 20 de junio de de 2007 – Grupo de Trabajo del Artículo 29 01248/07/ES WP 136

32 David Vernet y Xavier Canaleta - "La biometría y su legalidad" consultable en http://www.salle.url.edu/~dave/papers/jis2004a.pdf

e) *Verificación de patrones oculares*: De los métodos más efectivos (retina e iris) por la misma razón que la huella dactilar. No goza de buena aceptación de parte de los usuarios, por su carácter invasivo (escaneo del ojo) y por la posibilidad de dejar al descubierto cuestiones íntimas o privadas (consumo de drogas o alcohol, padecimiento de alguna enfermedad).

f) *Reconocimiento facial*: es una aplicación dirigida por un programa informático para identificar automáticamente a una persona en una imagen digital, mediante la comparación de determinadas características faciales, a partir de una imagen digital o un fotograma de una fuente de vídeo. Una de las maneras de hacer esto es mediante la comparación de determinados rasgos faciales de la imagen facial y una base de datos (extraido de la *Wikipedia*).

- II -

Existen dos funciones distinguibles de la biometría, que son la verificación y la identificación.

La verificación consiste en comparar una muestra biométrica de la persona con los datos registrados que se poseen de la misma. Para reforzar la precisión de concordancia que aporta esta técnica, se utilizan varios tipos de datos al mismo tiempo, por ejemplo la huella dactilar y el iris. Se desencadena así un tipo de control de identidad basado en datos de una única persona, que son objeto de un proceso automatizado.

La identificación supone la comparación de datos del sujeto a identificar, no solamente con sus propios datos registrados sino también con los datos registrados de otros sujetos. Por definición ya no es posible, como en el caso anterior, conservar los datos registrados exclusivamente en un soporte de almacenamiento individual. La concordancia es, en este caso, con datos provenientes de varias personas. La técnica permite concluir que el sujeto en examen utiliza varias identidades, o está tratando de ocultar la propia bajo el nombre de otra persona (usurpación de identidad).

La selección de datos a almacenar, y la elección de una u otra función no son aspectos irrelevantes para el derecho de la protección de datos personales. La vía elegida debe respetar el principio de proporcionalidad, buscando no sobredimensionar las prestaciones y exigencias del sistema por encima de la finalidad perseguida con la captura y tratamiento del dato. En pocas palabras, no es necesario almacenar otros datos biométricos que aquellos estrictamente necesarios a la finalidad perseguida por el instrumento que se trate (pasaporte, documento de identidad, visado, etc.). Y los procesos desencadenados deben limitarse también a la función menos invasiva (verificación), cuando no aparece justificado abarcar la función más invasiva (identificación).

El elemento biométrico para servir a un sistema con las finalidades apuntadas, debe ser **universal** (existe en todas las personas), **único** (debe ser distintivo para cada persona) y **permanente** (se mantiene a lo largo del tiempo).

Otra clasificación de importancia de las técnicas biométricas es la que distingue según utilicen datos estables (físicos y fisiológicos) o datos dinámicos (comportamiento). Ejemplos de los primeros son la comprobación de las huellas digitales, el análisis de la imagen del dedo, reconocimiento del iris, etc. Ejemplo de los segundos, la comprobación de la firma manuscrita, el análisis de la pulsación sobre las teclas, el análisis de la forma de caminar, etc.

Otra cuestión igualmente importante, en este caso ya de cara a la protección de datos, es la forma de almacenamiento de las plantillas personales, que depende del tipo de aplicación para el que se vaya a usar el dispositivo y el tamaño de las propias plantillas. Estas plantillas se pueden almacenar en: la memoria de un dispositivo biométrico, una base de datos central, o en tarjetas (plástico, ópticas, inteligentes). Este último método permite a los usuarios portar con ellos sus plantillas, como dispositivos de identificación.

- III -

En el pasado la utilización de esta tecnología se limitaba a sectores acotados y especializados como la investigación criminal. Pero luego se fue generalizando y extendiendo a numerosas aplicaciones, tanto del sector público como privado. Un proceso de masificación de esta técnica, puede conducir también a la banalización de los aspectos jurídicos y éticos en juego, lo cual se evita con posturas de precaución y garantía de los procesos desencadenados con la aplicación de esta técnica.

Como quiera que sea, los sistemas biométricos continúan expandiéndose a múltiples efectos. La internacionalización de la sociedad humana planetaria, con el incremento considerable de los desplazamientos de las personas, el avance en las facilidades y prestaciones que ofrece la técnica para agilizar los controles fronterizos, y el aumento superlativo de las medidas de policía y seguridad adoptadas por los Estados para frenar la escalada del terrorismo y la delincuencia internacionales, son otros tantos factores que han determinado que entidades internacionales y Estados se hayan ido abriendo cada vez más al uso de este tipo de técnicas, como forma de identificación, seguimiento y/o control de individuos, sus movimientos y actividades.

Como toda tecnología relacionable con la identificación y seguimientos de las personas, la biometría presenta riesgos de vulneración de los derechos y libertades fundamentales. La integridad del cuerpo humano, la manera en que se lo utiliza a fines técnicos, son cuestiones que se relacionan directamente con la dignidad humana. Por lo tanto, la adopción de este tipo de sistemas, su instru-

mentalización, el personal afectado a ello, conlleva aspectos éticos y jurídicos de cuidado y requerida consideración.

El respeto del cuerpo humano tiene vinculación estrecha con el derecho al respeto de la vida privada e intimidad de las personas. En los procesos de recolección y utilización de características del cuerpo humano están en juego la dignidad humana. Las nuevas técnicas no deben servir para aumentar desigualdades ni discriminaciones. Los problemas en el horizonte son múltiples: uno de ellos es que el dato biométrico revela datos sensibles aún cuando no sea la finalidad perseguida (ej. enfermedad, discapacidad).

En este orden de consideraciones, comenzaremos por analizar cómo y en qué medida, la incorporación de elementos biométricos en documentos de identidad y pasaportes se adecúan a la Ley Nº 18.331, y al sistema jurídico protector en su conjunto.[33]

- IV -

Por principio, la recolección y tratamiento de datos personales cualquiera sea el soporte o técnica en la que se fundan y organizan, son actividades que deben enmarcarse dentro de los principios contenidos en la precitada Ley para considerarse lícitas y ajustarse en un todo a derecho.

Los datos biométricos no escapan a la enunciada regla. Se destaca para el caso en examen la necesidad de aplicación y cumplimiento de los siguientes principios:

A) Finalidad o justificación para utilizar este tipo de datos, modificando sistemas tradicionales imperantes hasta el momento (arts. 5 literal C y 8).

B) Proporcionalidad, en cuanto a no solicitar ni emplear datos excesivos (o sea desconectados de la finalidad propuesta) al servicio de la nueva modalidad proyectada (la ley ubica este principio bajo al expresión "ecuánimes, no excesivos" en el art. 7).

C) Seguridad de la integridad de los datos obtenidos, que deberá ser de las más altas teniendo presente el tipo de tecnología e información en juego, volumen y fines de interés público que justifican el tratamiento (arts. 5 literal E y 10).

Podría llegarse a pensar que la recolección de datos de las características y fina-

33 El presente Informe se limitará al análisis exclusivo de este tipo de usos. La biometría se usa además (o se pretende usar y ha sido impugnado en ciertos casos del derecho comparado) en actividades de la esfera privada, vinculadas a franquear accesos de puertas que contienen dispositivos de seguridad, controlar horarios de trabajadores, entre otras posibles utilidades.

lidades a las proyectadas en el caso que motiva estas actuaciones, escapan a la aplicación de la Ley No. 18.331, en virtud de lo que ésta misma preceptúa en su art. 3 literal B. Sin embargo no es así sino que resulta producto de una apreciación superficial y equivocada sostener que por el solo hecho de tratarse de bases de datos (o aún datos sueltos que no llegan a conformar esta estructura) fuera del ámbito del marco legal de la materia, se está fuera de cualquier otra consideración jurídica. El funcionamiento global del sistema jurídico de protección de datos personales, por el contrario, debe ser entendido y asumido considerándolo en forma racional, completa y sistemática.

En efecto, el hecho de que no se le aplique la ley general de la materia a este tipo de bases de datos, no significa que queden al margen del sistema global, puesto que estando en juego -como están- derechos fundamentales consagrados por el art. 72 de la Constitución, será necesario en todo caso producir una interpretación armónica acerca de qué se le aplica y qué no se le aplica a este tipo de bases de datos, en materia de protección de datos personales, más allá de la letra legal.

Como bien lo enuncia el art. 1º de la Ley Nº 18.381 y se desprende también del llamado "bloque de constitucionalidad"[34], estamos ante un derecho "inherente a la persona humana" que rige en todos los campos, aún con limitaciones derivadas de razones de interés general (art. 10 de la Constitución) y sin necesidad de previsión ni reglamentación específica (arts. 72 y 332 de la Constitución).

Por lo tanto, parece ser indesmentible que, a pesar que la propuesta en examen encaja perfectamente en el art. 3 literal B de la Ley No. 18.381 (exclusión del ámbito de aplicación de la ley), de todos modos la carta de principios y derechos que simplemente enuncia (pero no la crea) la ley, resultan de aplicación necesaria y obligatoria también a este tipo de bases.

- V -

Corresponde pasar ahora al examen del derecho comparado, sobre normas, recomendaciones y criterios jurídicos relativos a la utilización de datos biométricos en pasaportes, cédulas de identidad y afines (ej. tarjetas migratorias), en directa relación con el derecho de protección de datos personales.

A nivel del Consejo Europeo existe un movimiento progresivo de apertura hacia este tipo de técnica, al propósito indicado. Se destacan como antecedentes más remotos la Resolución de 17 de octubre de 2000 estableciendo normas mínimas de protección de los pasaportes, y el Consejo Europeo de Salónica de 19 y 20 de junio de 2003 confirmando la necesidad de adoptar medidas comunes en materia de identificadores y datos biométricos para los documentos de los nacionales

34 Ver por todos Francisco Rubio LLORENTE - "El bloque de constitucionalidad" en http://www.cepc.es/rap/Publicaciones/Revistas/6/REDC_027_009.pdf

de los países terceros, los pasaportes de los ciudadanos de la UE y los sistemas de información.

También se menciona que la introducción de elementos biométricos en este tipo de documentos responde a la necesidad para los Estados miembros que forman parte del Visa Waiver Program de los EE.UU., de alinearse con la legislación americana a este respecto, para que sus nacionales puedan entrar en el territorio estadounidense sin visado.

El Reglamento (CE) Nº 2252/2004 del Consejo de Europa dicta normas en la materia, con modificaciones y especificaciones posteriores[35]. La norma comunitaria considera que la inserción de elementos biométricos en los pasaportes y documentos de viaje permitirá mejorar la protección de estos documentos e impedir su falsificación. Se postula que el aumento de la fiabilidad de los controles que verifican que las personas que presentan un documento son las mismas a las que se les ha expedido dicho documento, como la mejor manera de impedir la utilización de identidades falsas. A tales propósitos, los pasaportes y documentos de viaje incluirán un soporte de almacenamiento destinado a memorizar datos digitalizados, con capacidades suficientes para garantizar la integridad, autenticidad y confidencialidad de los datos. El soporte contendrá una imagen facial e impresiones dactilares.

Del punto de vista garantista el Reglamento establece lo siguiente:

- Finalidad exclusiva de comprobación de la autenticidad del documento e identidad de su titular.
- Derecho de comprobación de los datos personales inscritos con esta técnica, rectificación o supresión cuando corresponda, a favor del tenedor del documento.

La Comisión establecerá especificaciones técnicas complementarias en referencia a: medidas de seguridad adicionales (lucha contra la producción de documentos falsos); soporte de almacenamiento y su seguridad; requisitos sobre calidad y normas comunes relativas a la imagen facial y las impresiones dactilares.

La Propuesta de modificaciones de este Reglamento apunta al régimen observable en la materia para menores de 6 años: exoneración de facilitar impresiones dactilares y obligación de tenencia de pasaporte propio para control seguro de sus datos biométricos, lo que no ocurre si el menor está incluido en el pasaporte

35 Reglamento (CE) No. 2242/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros. Propuesta de modificación del Reglamento (CE) No. 2242/2004… Decisión de la Comisión de 28 de junio de 2006 por la que se establecen las especificaciones técnicas sobre las normas de las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros… Consultables en http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l14154_es.htm

de los padres. La Decisión de 28 de junio de 2006 completa el régimen con especificaciones técnicas extendidas en respectivos anexos, acerca de:

- elemento biométrico principal – Imagen facial;
- elemento biométrico secundario – Impresiones dactilares;
- soporte de almacenamiento;
- disposición electrónica del chip del pasaporte;
- cuestiones relacionadas con la seguridad y la integridad de los datos;
- valoración de la conformidad.

El Parlamento Europeo terminó dando luz verde a este Reglamento recogiendo parcialmente las modificaciones propuestas por el Consejo (ej. no utilización de huellas dactilares biométricas de menores 12 años).[36]

Otro documento destacable en la materia es el "Informe del Consejo de Europa" elaborado por el T-PD en su 21ª reunión (2-4 de febrero de 2005). Este informe comienza por alertar la necesidad de adoptar una posición respecto a la aplicación de los principios de protección de datos a este campo, con el propósito de contribuir a los debates y proyectos en curso a escalas nacionales e internacionales[37]. Luego de un minucioso examen del tema, el Informe concluye en la pertinencia, por sus virtudes intrínsecas, de la aplicación de los Principios jurídicos contenidos en la Convención 108 al campo de los sistemas que utilizan la biometría, a pesar que muchas cuestiones siguen estando abiertas y que ha habido avances tecnológicos considerables desde la redacción de la Convención.

A modo de resumen, este Informe destaca 12 conclusiones:

- La necesidad de considerar los datos biométricos como una categoría específica de datos en la medida que proceden del cuerpo humano y se trata de datos que siguen siendo los mismos en distintos sistemas, siendo inalterables de por vida sin perjuicio de eventuales cambios, por ejemplo por envejecimiento o intervenciones quirúrgicas.
- La necesidad de que el responsable del proceso evalúe las ventajas e inconvenientes posibles para la vida privada de la persona afectada del hecho de introducir este tipo de sistemas, sus finalidades y posibles soluciones alternativas que supongan un menor atentado contra la vida privada.
- Consideración de los aspectos socioculturales y posibles reticencias respecto del uso instrumental del curso humano, no optándose por la biometría solo

36 Consultable en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20090114IPR46171+0+DOC+XML+V0//ES A modo de resumen, en http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142555270427&esArticulo=true&idRevistaElegida=1142554112855&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales

37 Informe de situación relativo a la aplicación de los principios de la Convención 108 a la recogida y al proceso de los datos biométricos – Estrasburgo, febrero de 2005 (Traducción al español NO OFICIAL realizada por la Agencia Española de Protección de Datos del documento original en inglés), consultable en https://www.agpd.es/portalweb/canaldocumentacion/textos_interes/common/pdfs/informe-principios-convencion-108.pdf

por el hecho de que su uso resulte práctico.

- Utilización de los datos biométricos y demás datos asociados generados por el sistema, con fines determinados, explícitos y legítimos, no debiendo ser procesados luego de modo incompatible con estas finalidades.
- Carácter adecuado, pertinente y no excesivo de estos datos en comparación con la finalidad del proceso. Limitación de la recogida.
- Elección motivada entre almacenamiento solamente en un soporte individual, en una base de datos descentralizada, o en una centralizada, a la luz de los aspectos de seguridad.
- Estructura proporcional del sistema biométrico respecto a la finalidad del proceso. Si basta con el propósito y resultado de verificación mediante patrones, se debe evitar la obtención y almacenamiento de la imagen biométrica; es decir que no debe irse más adelante para obtener una solución de identificación más allá de lo necesario.
- Información a la persona afectada sobre la finalidad del sistema y la identidad del responsable del proceso, datos procesados, y categorías de personas a las que se comunicarán, garantizando con ello la lealtad y transparencia del proceso.
- Vigencia de los derechos de acceso, rectificación, bloqueo y cancelación de datos a favor de la persona afectada. Se extiende a los posibles datos asociados (ej. fecha y localización del sistema utilizado), y personas a las que se hayan comunicado los datos.
- Previsión de medidas técnicas y organizativas adecuadas con el fin de proteger los datos biométricos y demás datos de carácter personal asociados, contra la destrucción accidental o ilícita, y la pérdida accidental, así como contra accesos, modificaciones, comunicaciones no autorizadas o cualquier otra forma de proceso ilícita.
- Desarrollo de un procedimiento de certificación y control, en especial en las aplicaciones en masa, para establecer normas de calidad informática (software y hardware), junto con la formación del personal responsable del registro y la verificación. Se recomiendan auditorías periódicas que prueben las cualidades técnicas del sistema.
- Medidas alternativas para los casos de rechazo del sistema biométrico a la persona afectada, e información al afectado en el mismo momento del supuesto no reconocimiento por el sistema.

- VI -

A nivel de Grupo de Trabajo Artículo 29 existen varios estudios sobre el tema.

El Documento del Grupo de Trabajo Artículo 29 sobre "administración en línea" del 08-05-2003 resulta de interesante lectura por cuanto resume los distintos enfoques y niveles de avance de los países europeos, en la adopción de identificadores digitales únicos de personas, en contextos de facilitación del gobierno electrónico que –si bien son más amplios- incluyen la temática en examen.

De la lectura de este documento se extrae que en el concierto de naciones europeas no existe consenso sobre el tema[38]. El panorama es variado: mientras que algunos países han optado por sistemas de identificador único y general a escala nacional, otros han preferido identificadores sectoriales (seguridad social, pasaporte, impuestos…). En algunos de estos países conviven ambos sistemas, mientras que en Alemania y Portugal resulta inconstitucional recurrir a un identificador único. En ciertos casos se aprecian debates, incluso fuertes, acerca del riesgo de generalización de identificadores sectoriales. Finlandia previó un proyecto de revisión de estos sistemas en el contexto de la administración en línea, recurriendo a un solo identificador único creado especialmente para funciones de firma electrónica e identificación ante el Centro de registro de la población, pero no previendo que se use para acceder a los procedimientos en línea. En Bélgica, según informa el Documento, el avance de la administración en línea determinó la creación de un identificador único para empresas en relación con todos los sistemas de información de las autoridades públicas, que es el número de IVA (sic), ampliado a empresas y organizaciones exentas.

Más específicos en cuanto a régimen y previsiones aconsejables, resultan el WP 80[39] y el WP 112[40]. La importancia de ambos documentos en términos de orientación global hacia previsiones en este nuevo campo, aconseja un minucioso comentario al respecto.

WP 80 – Documento de trabajo sobre biometría

El Documento de trabajo sobre biometría (WP 80) introduce el tema, hace una descripción de los sistemas biométricos, aplica los principios de la Directiva 95/46/CE a este nuevo tipo de datos, establece criterios de legitimación para el tratamiento de estos datos y culmina con algunas conclusiones.

El documento se propone contribuir a la aplicación eficaz y armoniosa a los sistemas biométricos, de las disposiciones nacionales adoptadas de acuerdo con la Directiva 95/46/CE. Se establecen las dos funciones de estos sistemas: autenticación/comprobación una de ellas, identificación la otra. Se ubica claramente el debate a escala planetaria sobre la introducción de la biometría en carnets de identidad, pasaportes, documentos de viaje y visados, a partir de los sucesos del 11 de septiembre de 2001.

La Directiva 95/45/CE, nos reseña el WP 80, define los "datos personales" como

38 WP 73 – Documento de Trabajo sobre la administración en línea, adoptado el 08.05.2003. Consultable en http://www.informatica-juridica.com/anexos/anexo539.asp

39 WP 80 – Documento de trabajo sobre biometría, adoptado el 01-08-2003. Consultable en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_es.pdf

40 WP 112 – Dictamen 3/2005 sobre la aplicación del Reglamento (CE) nº 2252/2004 del Consejo, de 13 de diciembre de 2004 sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros. Consultable en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_es.pdf

"toda información sobre una persona física identificada o identificable", y agrega que se considerará identificable toda persona cuya identidad pueda determinarse, directamente o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de identidad física, fisiológica, psíquica…". El Considerando 26 añade como explicación que "para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento *o por cualquier otra persona,* para identificar a dicha persona". Por lo tanto, las medidas de identificación biométrica o su versión digital en forma de plantilla, normalmente serán "datos personales".

En otras palabras, los datos biométricos son datos personales en la medida que afecta o se vinculan con elementos informativos de una persona determinada, y las propias funciones de esta técnica avalan lo expresado: distinguir un individuo como diferente de otros (lo que se denomina autenticar/comprobar) e identificar.

Se hace especial mención y análisis extensivo de los siguientes principios contenidos en la Directiva: fines y proporcionalidad; obtención leal e información al interesado; consentimiento del afectado cuando el mismo es exigido por norma jurídica o el responsable del tratamiento del registro lo utiliza como motivo de legitimidad.

El Grupo Artículo 29 apoya el uso de sistemas biométricos que no memoricen rastros en un dispositivo de control de acceso, ni los almacene en una base de datos central. Pero si de todos modos se utilizan estos últimos (con el consiguiente aumento de riesgo en la seguridad) el Grupo recomienda que los Estados miembros contemplen la posibilidad de presentarlos al control previo por parte de las autoridades encargadas de la protección de datos, de conformidad con el art. 20 de la Directiva.

En cuanto a "medidas de seguridad", el responsable del tratamiento deberá tomar todas las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción y otro tipo de alteraciones, pérdidas o difusiones no autorizadas, en particular cuando el tratamiento incluya la transmisión de datos biométricos dentro de una red. Ejemplos de tales medidas: la codificación de las plantillas, la protección de las claves de codificación, el bloqueo de una ingeniería inversa, etc.

Ciertos datos biométricos podrán considerarse "datos sensibles", en particular los que revelen origen racial o étnico, o los relativos a la salud. El art. 8 de la Directiva prevé garantías adicionales al respecto (derecho a impugnar decisiones automatizadas discriminantes).

WP 112 – Dictamen 3/2005 sobre la aplicación del Reglamento (CE) nº

2252/2004 (medidas de seguridad y datos biométricos en pasaportes y documentos de viaje expedidos por Estados miembros

Retoma los análisis del WP 80, reseña antecedentes de tratamiento del tema a nivel europeo, y circunscribe el análisis a la obligatoriedad de incluir una imagen facial digitalizada e impresiones dactilares como elementos biométricos de los pasaportes de los ciudadanos de la UE (cf. Reglamento nº 2252/2004).

Comenta las consecuencias de gran envergadura de este precepto (que habría entrado a regir en 2009 luego de la aprobación del Parlamento Europeo), tratándose de datos que pueden almacenarse en bases de datos y quedar disponibles para muchos fines no previsibles.

Se señalan los riesgos éticos, aludiendo al Proyecto BITE (ética de la tecnología de la identificación biométrica) financiado por la CE[41]. Deberían implantarse y usarse, se expresa, procedimientos accesorios para favorecer a las personas que no puedan seguir con éxito el proceso de registro, y para evitar que sean ellas quienes deban soportar la carga de las imperfecciones del sistema, teniendo presente que los datos biométricos no son ni accesibles a todos ni del todo exactos. Hay debates científicos que no se pueden pasar livianamente por alto, como el de la dependencia de algunos dibujos papilares (huellas dactilares) de la nutrición del feto durante el tercer mes de embarazo. Y hay otros… que reseña el documento.

Como aspectos netamente legislativos se señalan: la resistencia fundada a permitir bases de datos centrales de pasaportes y documentos de identidad en general, por el riesgo de que infrinja el principio básico de proporcionalidad, y el favorecimiento del uso indebido; el acceso a la biometría únicamente a las autoridades competentes.

Como aspectos técnicos, y siempre atendiendo los riesgos que conllevan estos sistemas, se señala el de la implantación de un chip sin contacto (chip RFID) y la inclusión de elementos biométricos contenidos en ese fin. En su Decisión legislativa de 2 de diciembre de 2004 el Parlamento Europeo solicitó que el pasaporte incluyera un soporte de almacenamiento muy seguro, con la suficiente capacidad y apto para salvaguardar la integridad, autenticidad y confidencialidad de los datos almacenados. El Grupo apoyó la iniciativa, pero ello no fue tenido en cuenta por el Consejo. Se señala que el chip RFID conforme norma ISO 14443 previsto por el Reglamento de 13 de diciembre de 2004 crea muchos riesgos para el derecho a la intimidad de los ciudadanos europeos; y que la Decisión de la Comisión de 28 de febrero de 2005 no es adecuada para proteger los derechos de los ciudadanos, pues el contacto entre el chip RFID y el aparato lector puede ser objeto de interferencias y la información puede ser observada. Y las críticas

41 http://www.biteproject.org/

continúan respecto a las tecnologías específicas asumidas por el Reglamento y documentos afines, en cuanto a la falta de seguridad (implantación de una imagen facial digitalizada, e inclusión de elementos biométricos adicionales, particularmente huellas digitales.
Las 6 conclusiones del WP 112 son contundentes. Las resumimos a continuación:

Acápite: la inclusión de elementos biométricos en pasaportes, otros documentos y carnés de identidad, plantea muchas cuestiones éticas, legales y técnicas.

1) Antes de introducir estos elementos, deberá tener lugar un debate exhaustivo en la sociedad, y para ello es necesario aguardar los resultados del proyecto BITE.

2) Para limitar los riesgos se deben introducir garantías eficaces desde un primer momento, a tenor de lo que establezcan los expertos.

3) Debe garantizarse la estricta distinción entre datos biométricos recogidos y almacenados a efectos públicos (ej. control fronterizo) que operan sobre la base de obligaciones legales, y datos utilizados a fines privados, de base contractual requirente del consentimiento.

4) Necesidad de restringir técnicamente el uso de la biometría en pasaportes y documentos de identidad a efectos de verificación (comparación de los datos del documento con los datos proporcionados por el titular al presentar el mismo).

5) Garantizar que los pasaportes de ciudadanos europeos que no incluyan datos de las huellas dactilares no puedan ser leídos por lectores que no apliquen el Control de Acceso Ampliado.

6) Garantizar que solo las autoridades competentes pueden tener acceso a los datos almacenados en el chip.

- VII -

La 27ª Conferencia Internacional de Comisarios de Protección de Datos y Privacidad (Montreux, 16 de setiembre de 2005) emitió una "Resolución sobre el uso de la biometría en pasaportes, tarjetas de identidad y documentos de viaje" informando en sus considerandos algunos de los riesgos que conlleva esta tecnología, tales como que se generen datos biométricos personales sin que el ciudadano se de cuenta de ello, así como la posibilidad de que el cuerpo humano se convierta en un identificador universal legible a través de máquinas.

En base a estos riesgos, la Resolución reclama en su parte dispositiva lo siguiente:

garantizar contra los riesgos presentes en esta tecnología para lo cual se requiere la adopción de medidas eficaces desde las primeras fases de implementación de estos sistemas; distinción estricta entre su aplicación con fines públicos (ej. controles fronterizos) con arreglo a obligaciones legales, y fines contractuales basados en el consentimiento; limitación de su uso con fines comparativos entre los elementos de esta naturaleza contenidos en el documento y los datos ofrecidos por el titular en el momento de presentarlo.

En España la legitimación para el tratamiento de datos del DNI (Documento Nacional de Identificación) se encuentra en la Ley Orgánica 1/1992 de 21-02-1992 sobre Protección de la Seguridad Ciudadana. La norma preceptúa que la tenencia del DNI es un derecho de todos los españoles al tiempo que una obligación legal para personas mayores de 14 años. La misma ley establece los datos que se deben incorporar, si bien permite su mayor determinación a través de normas reglamentarias.

En particular el DNI electrónico se encuentra habilitado formalmente por la Ley 59/003 de 19-12-2003 sobre firma electrónica, donde se establece que el mismo *"se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. La ley se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus dos notas más características -acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico."*[42].

Sobre el respeto del principio de finalidad en el caso del DNI electrónico español, y otras características del mismo, ha expresado el anterior Director de la Agencia Española de Protección de Datos lo siguiente: *"En cuanto al principio de finalidad regulado y exigido por la Ley Orgánica de Protección de Datos, la Ley de Firma Electrónica configura el DNI electrónico como el documento de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos. En lo que se refiere a los datos objeto de tratamiento, la proporcionalidad del mismo y la seguridad, el DNI electrónico se basa en una tarjeta inteligente que contendrá grabados en el soporte físico los mismos datos de filiación del ciudadano que figuran en el documento de identidad actual o convencional. Además, dispondrá de un chip con capacidad criptográfica embebido en el material de la tarjeta. La información contenida en este chip estará fraccionada en tres zonas, cada una de ellas con unos requisitos de acceso y seguridad diferentes: Zona privada, accesible exclusivamente por el titular del documento mediante clave de paso o clave de acceso; zona pública, accesible sin restricción, y zona restringida, con el fin de que las Fuerzas y Cuerpos de Seguridad del Estado puedan comprobar que no se ha alterado*

42 Exposición de motivos de la Ley No. 59/003 de 19-12-2003, consultable en http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=2003/23399

la información contenida en el soporte físico. En esta área se contienen los datos biométricos del ciudadano".[43]

El Real Decreto 1553/2005 de 23-12-2005, finalmente, reglamenta la Ley Orgánica 1/1992 y establece que el chip incorporado en la tarjeta soporte contendrá los siguientes datos: (art. 11.3)

- Datos de filiación del titular
- Imagen digitalizada de la fotografía
- Imagen digitalizada de la firma manuscrita
- Plantilla de la impresión dactilar del dedo índice de la mano derecha, o en su caso, del que corresponda según lo indicado en el art. 5.3 de ese Real Decreto.
- Certificados reconocidos de autenticación y de firma, y certificado electrónico de la autoridad emisora, que contendrán sus respectivos períodos de validez.
- Claves privadas necesarias para la activación de los certificados mencionados anteriormente.

- VIII -
Conclusiones

1) Los sistemas biométricos configuran una tecnología capaz de cumplir dos funciones, la primera menos invasiva que la segunda: A) Verificar la existencia de determinadas propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, atribuibles a una sola persona y mensurables. B) Identificar al sujeto del cual se poseen sus datos biométricos, por comparación con éstos y eventualmente también con los datos biométricos de terceros sujetos.

2) En el actual estado de la técnica, existen los siguientes tipos de sistemas biométricos: A) Verificación de escritura manuscrita o firma. B) Verificación de huellas dactilares. C) Verificación de patrones de la mano. D) Verificación de la voz. E) Verificación de patrones oculares. F) Reconocimiento facial.

3) En procesos como los analizados, que suponen la recolección y utilización de características del cuerpo humano, entran en juego el respeto de dignidad humana, la vida privada e intimidad de las personas. La selección de datos a almacenar, y la elección de una u otra función, e incluso la elección de los soportes para contener este tipo de datos, no son aspectos irrelevantes para el derecho de la protección de datos personales.

43 Comparecencia del Director de la Agencia Española de Protección de Datos (Piñar Mañas) ante el Congreso de Diputados de España para informar sobre la Memoria de la Agencia Española de Protección de Datos del año 2004, a petición propia (número de expediente 212/000674). Recogido en Actas de fecha 29-09-2005 – Nº 353, consultable en https://www.agpd.es/portalweb/canaldocumentacion/comparecencias/common/pdfs/Comparecencia_Director_congreso.pdf El compareciente endicha oportunidad explica otros aspectos del sistema de firma electrónica y su relacionamiento con el DNI electrónico: funciones básicas del sistema, especies de datos personales incluidos en cada certificado digital, habilitaciones legales adicionales (posibilidad de incorporar el permiso de conducir y el documento que permite visualizar el saldo de puntos del mismo conforme apartado 23 de la Ley 17/2005 de 19-06-2005)

4) Por lo tanto, el asunto que convoca a su examen en este expediente refiere en última instancia a una proyección de actividades de recolección y tratamiento de datos personales, donde habrán de respetarse los principios de finalidad o justificación, proprocionalidad y seguridad, de conformidad con lo preceptuado en los arts. 5 lierales C y E, 7, 8 y 10 de la Ley Nº 18.331.

5) Al respecto es del caso tener presente que desde el año 2000 en adelante, en el derecho comunitario europeo surge un movimiento de apertura tendiente a la aceptación de la inclusión de elementos biométricos en documentos de identidad, pasaportes oficiales, y otros documentos de viaje. Movimiento no exento de opiniones críticas fundamentalmente basadas en que se estaría ante una tecnología que no es totalmente segura en sí misma. Y que se acentúa a partir del ataque terrorista de las Torres Gemelas.

6) Tal como plantea, entre otros, el Grupo del Artículo 29 en su WP 112, la inclusión de elementos biométricos en este tipo de documentos plantea cuestiones éticas, legales y técnicas, que obligan a tomar los siguientes recaudos:

   a) Debates exhaustivos previos, teniendo presente los resultados del llamado "proyecto BITE".
   b) Introducción de garantías eficaces desde el primer momento de implementación técnica y conforme lo establezcan los expertos.
   c) Distinción estricta entre datos biométricos recogidos y almacenados a efectos públicos (operativa legal), y datos utilizados a fines privados (operativa contractual con base al consentimiento del afectado).
   d) Restricción del uso de la biometría en pasaportes y documentos de identidad a efectos de verificación.
   e) Apoyo a la extensión del sistema comnocido como "Control de Acceso Ampliado".
   f) Garantizar que solamente las autoridades competentes puedan tener acceso a los datos almacenados en el chip.

Firmado por Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 92 de 19 de octubre de 2009.- Se informa sobre la regulación de las guías telefónicas conforme la Ley N° 18.331

Montevideo, 19 de octubre de 2009

Informe N° 92
Ref. Regulación de las Guías Telefónicas

Antecedentes

La consulta formulada a efectos de analizar el carácter de fuente pública de las guías telefónicas emitidas con anterioridad y posterioridad a la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP).

Regulación en el derecho comparado

I) Unión Europea

A nivel de la Unión Europea el tema de las guías telefónica ha sido regulado mediante la Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Es así que se establece dentro de sus considerandos que "*Deben armonizarse las disposiciones legales, reglamentarias y técnicas adoptadas por los Estados miembros para proteger los datos personales, la intimidad y los intereses legítimos de las personas jurídicas en el sector de las comunicaciones electrónicas, a fin de evitar obstáculos para el mercado interior de las comunicaciones electrónicas de conformidad con el artículo 14 del Tratado*".

Específicamente el artículo 12, sobre guías telefónicas, considera que tanto el derecho a la intimidad de las personas físicas como el interés legítimo en el caso de las personas jurídicas, hacen posible que los abonados puedan decidir si se hacen públicos sus datos personales en una guía, y en caso de prestar su consentimiento, determinar cuáles de ellos.

Complementariamente se establece el derecho de los usuarios a la no inclusión, comprobación, corrección o supresión de datos personales en forma gratuita.

Asimismo se establece que los suministradores de guías telefónicas deben infor-

mar a los abonados sobre la finalidad de éstas así como de cualquier otro tipo de uso particular que pueda hacerse con ellas.

Se regula que se debe informar si los datos puedan ser transmitidos a terceros y determinar quienes pueden ser éstos. Estos terceros solo podrán utilizar los datos para los fines para los cuales se recogió el consentimiento debiendo volver a recoger éste cuando se quiera utilizar para otras finalidades, el que puede ser recabado por el titular o por el tercero.
Asimismo este régimen se podrá hacer aplicable a las personas jurídicas de acuerdo a lo que establezcan las regulaciones nacionales.

El Grupo de Trabajo sobre Protección de Datos Personales – Artículo 29 se ha expedido sobre el tema en su Dictamen 5/2000, de 13 de julio de 2000, sobre el uso de las guías telefónicas públicas para servicios de búsqueda inversa o multicriterio.

Es así que establece que "*el fin de las guías telefónicas convencionales es revelar el número de teléfono de un abonado a partir del conocimiento del nombre de un abonado (…). Y el uso de los datos personales se limita a ese fin específico. Por lo tanto, utilizar las guías para averiguar datos personales relativos a la persona física a partir de un número teléfono cuyo abonado es desconocido…constituye un uso totalmente diferente del que el consumidor puede esperar cuando se le incluye en la guía (…)*".

II) Derecho Español

En España, la Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999 incluye a texto expreso los repertorios telefónicos cuando en el literal J) del artículo 3, define "Fuentes accesibles al público":

"Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación".

III) Latinoamérica

A nivel latinoamericano tenemos que tener presente la regulación de las guías telefónicas que se hace en Chile. El Reglamento de Servicio Público Telefónico aprobado por Decreto 425 de 09 de agosto de 1997 y modificado posteriormente establece en su art. 39 que ***"****La compañía telefónica local debe disponer en todo momento, en los medios que estime pertinentes, para todos los suscriptores*

que expresamente así lo requieran y sin costo para éstos, de una guía telefónica actualizada con la numeración telefónica vigente y en servicio. Ésta debe especificar el nombre, dirección donde se suministra el servicio y número de abonado, de todos los suscriptores locales de la zona primaria correspondiente. (...)
La inserción en la guía telefónica de la información relativa al suscriptor local la efectuará la compañía telefónica local sin costo para éste. El suscriptor local podrá solicitar la inserción a nombre de terceros, sin que ello implique el traspaso de la calidad de suscriptor. Dicha inserción debe, además, ser autorizada por la persona cuyo nombre aparecerá en la guía telefónica.
La compañía telefónica local debe disponer de la información antes mencionada, actualizada mensualmente, para efectos de atender las consultas recibidas a través del nivel de informaciones.
Para estos efectos, dentro de los primeros 10 días de cada mes, cada compañía telefónica local deberá suministrar, a las demás compañías telefónicas locales y a solicitud de éstas, la siguiente información actualizada referida a sus suscriptores: nombre o razón social del suscriptor, dirección donde se suministra el servicio y número de abonado. Dicha información se debe suministrar, en medios magnéticos, ordenada alfabéticamente según el nombre del suscriptor y por zona primaria, o mediante otros medios que de común acuerdo establezcan las partes.
La información respecto de los suscriptores que hayan contratado con la compañía telefónica local el servicio de no publicar ni informar (NPNI) no se incluirá en la guía telefónica, no se informará a través de los niveles de informaciones y no se traspasará a otras compañías telefónicas locales".

En Argentina, se consideran que los datos que figuran en la guía son públicos y por tanto no requieren de consentimiento. A su respecto se ha dicho que: *"Hay toda una serie de datos que aunque no son problemáticos en soporte papel, pues su posterior recuperación resulta un tanto compleja, sí lo son cuando pasan a estar en formato digital, al ser absurdamente fácil cruzarlos, además de posibilitar la recuperación rápida y eficiente de los mismos. Consideremos los números de teléfono. No es relevante que esté en un formato papel, accesible a todo el mundo, la guía telefónica, pues si alguien sabe el nombre de la persona que busca podrá encontrar su número de teléfono, lo que resulta hasta cierto punto razonable. Pero si esa misma información está en formato digital, es fácil hacer búsquedas cruzadas y saber quién soy a partir de mi número de teléfono o, cruzando datos con alguna otra base de datos, saber donde vivo y ser víctima del agobiante Telemarketing".* (Universidad de Buenos Aires, Facultad de Derecho y Ciencias Sociales – Actualización en Derecho Informático, año 2000). (subrayado de las informantes)

IV) Nuestra legislación – Ley N° 18.331

El artículo 9° de la Ley N° 18.331 que regula el principio del previo consentimiento informado detalla que este debe ser libre, previo, expreso y que deberá documentarse. Prevé que no será necesario, entre otras hipótesis, cuando:
"A) Los datos provengan de fuentes públicas de información, tales como registros o

publicaciones en medios masivos de comunicación.(...)
B) 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".

El artículo 4° de la LPDP define fuentes accesibles al público, como aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. (literal i).

Nuestra LPDP y su decreto reglamentario nada dicen acerca de qué condición revisten las guías telefónicas. En efecto, solo se alude a que no se necesitará el previo consentimiento en los listados que contemplen nombres y apellidos, domicilios, etc., dejando fuera entonces los números telefónicos.

Análisis

Al amparo de lo dispuesto en el artículo 9° de la LPDP, literal C), hay que diferenciar dos aspectos:

- los números telefónicos de las personas jurídicas, que no requieren el previo consentimiento informado.
- Los números telefónicos de las personas físicas, que sí requieren el previo consentimiento informado.

En efecto, a partir de la LPDP, el número telefónico de las personas físicas es un dato personal que requiere el previo consentimiento informado, de manera que cuando una persona contrata el servicio telefónico, el ente responsable deberá recabar el previo consentimiento del titular para incorporar ese número en una guía telefónica, sea ésta en formato papel o electrónica. El consentimiento deberá recolectarse, de forma gratuita, en las condiciones previstas por el artículo 9°, esto es, de forma previa, expresa, informada, el que deberá documentarse.

Ahora bien, con anterioridad a la sanción de la LPDP la situación era otra. Por años las guías telefónicas, contemplativas de nombre, domicilio y teléfono fueron consideradas como fuentes públicas de información; y quien solicitaba un servicio telefónico era sometido únicamente a la interrogante de si deseaba o no exclusión de guía, cobrándosele un monto estipulado por la negativa a su inclusión.
Es decir, consuetudinariamente las guías telefónicas emitidas hasta la fecha de sanción de la LPDP fueron consideradas fuentes públicas de información, siendo consultadas diariamente con ese carácter por empresas privadas, entes públicos y particulares en general.

La información contenida en cada guía telefónica en formato papel estaba a disposición de cualquier persona que deseara acceder. Esto es, a disposición del público en general, con la particularidad que el ente responsable de su emisión, ya no tenía posibilidades de control sobre esa "base de datos", puesto que ésta se encontraba en cada hogar, empresa u organismo público.

Dichos repertorios telefónicos se emitían anualmente o cada dos años, existiendo al día de hoy múltiples ejemplares, de los años que se deseen consultar, en cualquier domicilio particular, empresa o entidad pública, en cualquier punto del país.

Si bien, la LPDP dispone en su artículo 46 que las bases de datos deberán adecuarse a sus disposiciones dentro del plazo de un año de su entrada en vigor, las guías telefónicas (bases de datos de acuerdo a la definición que brinda el artículo 4°, literal A de la Ley), merecen un tratamiento disímil.

Desconocer este extremo y pretender adecuar las guiás telefónicas emitidas hasta la fecha de sanción de la LPDP, recabando el consentimiento de los titulares del servicio telefónico, a efectos de validar las guías telefónicas que por millares se encuentran en circulación, escapa a toda lógica y contraría la realidad fáctica.

Conclusiones

De lo expuesto se extrae que en mérito a la costumbre, tomando en consideración las soluciones del derecho comparado, y aplicando el principio de realidad, corresponde considerar a las guías telefónicas emitidas hasta el 11 de agosto de 2008 (fecha de sanción de la LPDP), como fuentes públicas de información.

A partir de la entrada en vigencia de la LPDP, para la emisión de nuevas guías telefónicas deberá recabarse previamente el consentimiento de los nuevos titulares del servicio telefónico, de acuerdo a lo consignado en el artículo 9° de la LPDP, cumpliendo con los requisitos allí contemplados.
Si bien se tiene conocimiento que en la actualidad la exclusión de guía ya no reviste el carácter de onerosa, deberá tenerse especial atención en la gratuidad del derecho de no inclusión.

Es todo cuanto tenemos que informar.

Firmado por Dra. Ma. José Rodríguez Tadeo y Dra. Flavia Baladán
Derechos Ciudadanos

Informe N° 118 de 9 de noviembre de 2009.- Se informa sobre consulta referida al alcance de los artículos 28 y 29 de la Ley N° 18.331

Montevideo, 09 de noviembre de 2009

Informe Nº 118/2009
Exp. Nº 2009/063: Consulta técnica sobre alcance de los arts. 28 y 29 de la Ley Nº 18.331

- I -

La consulta refiere a la interpretación y alcance del concepto de actividades exclusivamente personales o domésticas dentro de la sistemática de la Ley Nº 18.331.

No compartimos los argumentos vertidos por el consultante, reconociendo no obstante la valía de su elaboración como pieza de reflexión doctrinaria.

- II -

El derecho de la protección de datos personales se asienta en pocos decenios a esta parte como un derecho fundamental y autónomo, cuyo correcto entendimiento y alcances dependerá, al menos hoy día, de reconocer la necesidad de abrevar mayormente en las fuentes de derecho europeo, donde ha nacido y crecido como tal durante décadas, siendo un hecho incontrastable que no está aún totalmente consolidado entre nosotros.

Por tanto existe un deber de intérprete en cuanto a poner esfuerzo en trasvasar intelecciones meramente literales, y superar así posibles pequeñas imperfecciones de la norma nacional vigente, so pena de quedar anclados en minucias de entendimiento que siempre terminarán conspirando contra la institucionalidad de este derecho. Su instalación cultural aún se encuentra en ciernes entre nosotros, incluso en ámbitos especializados, lo que aconseja este tipo de posturas.

- III -

La tesis sustentada por la Unidad, de la que participa el suscrito, abreva en la fuente europea, donde existe un proceso de institucionalidad y asentamiento orgánico de este derecho que transita de larga data, aportando esclarecimientos aún ignotos para nosotros, fruto de la experiencia recogida en una evolución y profundización tanto dogmática como hermenéutica (el inicio de este colosal

proceso viene dado con las primeras leyes suecas y alemanas de principios de los años 70´del siglo pasado).

En este punto, y para ir de lleno al centro del asunto que plantea el consultante, debemos comenzar por consignar que la Directiva 95/46/CE se aparta notoriamente de dicho planteo. En la norma comunitaria se establece un ámbito muy concreto y estricto para lo que se denominan "actividades personales o domésticas", circunscribiéndolo a la personas físicas (art. 3.2. segundo guión y Considerando 12). Esto es muy claro, no admite dudas.

En la misma línea se encamina el Dictamen 4/2004 del "Grupo de Trabajo del Art. 29", en cuanto a que la excepción se aplica exclusivamente a actividades realizadas por personas físicas, no así jurídicas, dentro del marco de su vida privada y familiar.

También el TSJ de las CCEE, para el que "esta excepción debe interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada y familiar de los particulares" (caso Lindqvist, sentencia del 6 de noviembre de 2003).

- IV -

En el derecho español han sido varios los autores que han abordado y reflexionado sobre el punto.

Citaremos uno de ellos, VIZCAÍNO CALDERON[44], quien refiere al endurecimiento del régimen de la LOPD con respecto al de la anterior LORTAD en punto a la extensión de esta excepción. Mientras que en el régimen anterior se aludía a ficheros "mantenidos por personas físicas con fines exclusivamente personales", el régimen ulterior pasó a contemplar los "mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas", concepto más preciso -y por tanto más reduccionista del alcance de la excepción- que el primero.

La introducción del adverbio "exclusivamente" y su referencia ya no a "fines" sino a "actividades" hacen que no esté permitido excluir del ámbito legal las bases de datos mixtas, o sea aquéllas que contienen datos de uso personal o doméstico, pero también datos de uso profesional, empresarial, etc.

El Reglamento español profundiza este afán aclaratorio que ha presidido la evolución de la excepción de marras en el derecho español, con tres aclaraciones que caminan en esa dirección:

44 Miguel VIZCAINO CALDERON - *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Ed. Civitas, Madrid, 2001. Cit. por Juan Zabia de la Mata y otros - "Protección de Datos. Comentarios al Reglamento", Ed. Lex Nova, 2008, 956 págs. Ver "Google libros" de esta obra, págs. 81 a 84.

A) Recoge el mandato de la Directiva 95/46/CE, que incluye en la definición de la excepción "el tratamiento" de datos personales, cosa que no hace la LOPD (art. 2.2a de la LOPD, art. 4a primer párrafo del Reglamento).
B) Expresa de modo explícito que "actividades personales o domésticas" son las que "se inscriben en el marco de la vida privada o familiar de los particulares" (art. 4a. primer párrafo del Reglamento).
C) La expresión "particulares" utilizada, hace que queden fuera de la excepción los profesionales.

Igual conexión sobre lo que corresponde entender como "actividades personales o domésticas" y su vinculación de modo único a la esfera privada y familiar de los particulares, surge de la Instrucción 1/2006 de 8 de noviembre de la Agencia Española de Protección de Datos, relativa al tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras. El art. 1.3 de esta norma señala que escapa al ámbito regulatorio de la Instrucción "el tratamiento de imágenes en ámbitos personales o domésticos, entendiendo por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar". La norma es congruente con el Considerando 16 de la Directiva 95/46/CE en cuanto a que "los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública... o para el ejercicio de otras actividades que no están comprendidas en el ámbito de aplicación del Derecho comunitario".

- V -

Pretender que las personas jurídicas puedan poseer bases de datos para uso exclusivamente interno o personal significa tanto como exorbitar el concepto y alcance de estas ficciones legales, creadas y sometidas siempre al control estatal. Es lógico y racional que la persona jurídica sencillamente no tenga un "ámbito personal" en el sentido que corresponde utilizar en este campo. Otra cosa diferente es que se le aplique la ley en lo pertinente. He aquí la confusión inicial donde se asienta el nudo gordiano del planteo del consultante: la persona jurídica no posee, no puede naturalmente poseer, un ámbito personal al menos tal como es entendido a los efectos del régimen en aplicación.

Transitar por el andarivel propuesto por el consultante, implica sencillamente dejar en manos de los titulares de las empresas u otras personas jurídicas el cumplimiento o incumplimiento de la ley. Bastará con decir que tal o cual base de datos es de uso personal o interno para dejar de registrar una base de datos, y con ello dejar de cumplir la ley. Pero ¿quien resuelve lo que es o deja de ser "uso interno o personal" en una empresa? ¿Como se aplica este concepto a las personas jurídicas, ya que está bastante -por no decir totalmente- claro en el caso de las personas físicas, no así en el de las jurídicas?. Es sencillamente impracticable por la razón de fondo de que la propuesta no posee sustancia, carece de onto-

logía propia: no existe el uso personal o interno de las bases de datos, y si algo de ello hubiera en cierto momento, en otro momento diferente puede dejar de haberlo, y la misma base que supuestamente hoy fue declarada de uso personal o interno, mañana pasa a ser de uso abierto y externo porque al gerente de turno se le antojó hacerlo. No tiene ningún sentido admitir algo que rechina de tal modo a la realidad y simple obrar de la experiencia.
El reconocimiento y manifestaciones jurídicos de la "personalidad" en el caso de las personas jurídicas, asume y parte de fundamentos ciertamente dispares al de las personas físicas. Los controles existen siempre para las primeras, no necesariamente para las segundas. No hay un derecho fundamental a la protección de datos personales de la persona jurídica. Sus bases de datos, por el contrario, deben estar siempre sometidas al registro de la ley. ¿Porqué habrían dejar de estarlo si carecen de intimidad? Entre otras razones, las más pragmáticas apuntan a que nadie puede asegurar que lo que hoy es interno mañana deja de serlo. Y con eso se acaba la "historia" de esta "serpiente emplumada" denominada "ámbito personal individual o doméstico o interno de la sociedad" (conclusión del escrito de consulta), algo de lo que se podrá hablar pero resulta sencillamente inexistente.

Poca seriedad tendría el sistema proteccionista ideado en su conjunto, con tamaña fuente de fuga al cumplimiento de la ley. Si el derecho fundamental de protección de datos personales dependiera de que una empresa declare o no declare su base de datos, al abrigo de una consideración tan particular, maleable y discrecional como es la de considerar que algunas de esas bases de datos son de "uso personal o interno", sencillamente dejaríamos de tener un régimen jurídico justificado y especializado como tenemos. No se justifica. El sistema no fue ideado para ello. Y como tampoco se pueden comparar los alcances del dispositivo proteccionista destinado prioritariamente a la persona física en tanto a la persona jurídica la extensión del mismo es "en cuanto corresponda" (art. 2 de la Ley Nº 18.331), a nuestro juicio se cierra todo flanco de duda.

- VI -

Frente a esta clase de consideraciones como las que acabamos de exponer, entendemos que decaen los argumentos letristas que le podrían hacer decir a la Ley Nº 18.331 (y sus decretos reglamentarios) lo que estas normas no dicen.

No hay que confundir tampoco, como hace el consultante, algunos dispositivos de la Ley Nº 18.331 que consagran cierto excepcionamiento a fines parciales del sistema, con aquéllos que consagran el excepcionamiento a todo el sistema. En este rubro entran las "excepciones al consentimiento del titular de los datos", que desde luego tiene ese preciso alcance y no otro (art. 9 de la Ley), por lo que no por ello exonera a quien utiliza este tipo de informaciones para confeccionar una base de datos, de su deber de registrarla (arts. 6, 24 y 26).

Conclusión

1) La correcta interpretación del régimen jurídico creado en nuestro ordenamiento jurídico a partir de la Ley Nº 18.331, pero que en forma alguna debe desconectarse de la mayor tradición y profundización proveniente de otras latitudes (en particular la europea), no es la vertida por el consultante.
2) Al contrario de lo que sostiene, el verdadero entendimiento global y sistemático del régimen, conduce necesariamente a afirmar que no existen bases de datos de uso "personal", "individual" y/o "doméstico" de cargo de personas jurídicas.

3) Y en tal sentido, el texto del art. 15 literal B) segunda fase del Decreto Nº 414/009 de 31 de Agosto de 2009, es perfectamente congruente con el alcance de la norma legal, no verificándose la extralimitación alguna.

Firmado por Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 127 de 18 de noviembre de 2009.- Se informa sobre la procedencia o no del registro de determinadas bases de datos del Ministerio de Industria, Energía y Minería

Montevideo, 18 de noviembre de 2009

Informe N° 127
Ref.: Solicita no se proceda al registro ante AGESIC de las bases de datos de unidades administrativas del MIEM que dependen de otros organismos.

Antecedentes

El 12 de noviembre de 2009 se presentó ante la Unidad Reguladora y de Control de Datos Personales (en delante URCDP), el Ministerio de Industria Energía y Minería (MIEM) solicitando la opinión de la URCDP en relación con la persona responsable de la inscripción cuando se trata de bases interinstitucionales, administradas por organismos tales como la Oficina Nacional de Servicio Civil, el Ministerio de Economía y Finanzas y el Banco de Previsión Social (fs. 1).

Análisis

La presente consulta refiere a determinar si el MIEM es el responsable de la inscripción de determinadas Bases de Datos ante la URCDP.

A esos efectos, se debe definir qué es una Base de Datos. En ese sentido, el artículo 4 literal d) de la LPDP la define como *"indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso"*. En la consulta planteada se mencionan entre otros, los registros de becarios y los contratos a términos que conforman Bases de Datos. Por tanto, corresponde determinar quién es su responsable.

Para poder definir el estatus jurídico que ocupa el MIEM se debe determinar si existe un tratamiento y si éste se realiza para sí mismo o para otro organismo. En ese sentido, el literal M) de la LPDP define el tratamiento de datos como *"operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias"*.

De acuerdo a lo informado por el MIEM establece que *"…algunas unidades administrativas dependientes de este Ministerio acceden a dichos registros a efectos del ingreso de información,*

y en algunos casos, consulta,". (fs. 1). Por tanto, realiza un tratamiento de datos ya que procesan datos personales como puede ser por ej. el nombre, el teléfono, la dirección, etc. de las personas cuyos datos integran la Base de Datos de los contratados a término.

A efectos de determinar si estamos ante un responsable de tratamiento, debemos considerar que la LPDP define a éste como *"persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento".*

En este caso, el MIEM no es propietaria de la Base de Datos ni tampoco decide sobre su finalidad, contenido y uso del tratamiento, ya que la administración depende de otro organismo. Cabe concluir entonces que no se trata de un responsable.

Entonces surge la necesidad de determinar cuál sería su posición jurídica. En ese sentido se debe analizar si se trata de un encargado de tratamiento. Según la LPDP el encargado del tratamiento es aquella *"persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento"*. En este caso el MIEM, por una obligación normativa, trata datos personales de Bases de Datos que son, en principio de otros organismos.

Con respecto al destino del tratamiento de acuerdo a lo informado y a que se trata de Base de Datos cuya administración depende de otros organismos, la posición del MIEM sería una especie de encargado del tratamiento, ya que inserta información en una Base de Datos administrada por otro organismo. Es así que el MIEM en su escrito expresa que"*…lo cierto es que, como se dijo, han sido creados y su administración depende de otros organismos (…)"* (fs. 1)

La doctrina española, que se basa en una normativa que define en los mismos términos al responsable y al encargado del tratamiento, sigue esta postura estableciendo al respecto que *"Será encargado de tratamiento cuando la entidad en quien se delegue o se encomiende la gestión tributaria se limite a la recepción de los datos y la realización de las actividades necesarias para el efectivo cumplimiento de la relación jurídica tributaria, procediendo con posterioridad a devolver al Ayuntamiento la información previamente facilitada".* (Protección de Datos Personales para Administraciones Locales, pág. 70, Agencia de Protección de Datos de la Comunidad de Madrid).

A efectos de aclarar estos conceptos corresponde analizar la normativa que regula alguna de las bases de datos utilizada como ejemplos en su escrito, para definir cuál es la posición jurídica del MIEM ante la obligación de inscripción de las Bases de Datos.

Con respecto a la Base de Datos Sistema de Compras y Contrataciones Estatales (SICE), el artículo 1° del Decreto N° 232 de 09 de julio de 2003 establece que "*En los procedimientos de contratación directa previstos en el numeral 2 del artículo 33 del TOCAF y en el literal B) del numeral 3) de dicho artículo. los ordenadores del gasto deberán comunicar al Sitio www.comprasestatales.gub.uy , la información que se indica en el artículo siguiente, a los efectos de asegurar la publicidad del acto*".

Por ejemplo, la Base de Datos "Sistema de Compras y Contrataciones Estatales (SICE)", consigna que "*en ese mismo sentido, por Decreto 289/002, de 30 de julio de 2002, se establecieron las bases del Sistema de Compras y Contrataciones Estatales (SICE), al que deben enviar información todas las unidades de compras de la Administración Central, incluso aquéllas que cuentan con un sistema propio de compras y contrataciones, las que deben proveer al Comité Ejecutivo Para la Reforma del Estado (CEPRE) de la información requerida. Asimismo, el artículo 65 de la Ley N° 17.556 de 18 de setiembre de 2002 dispuso que el incumplimiento por parte de los Directores de las Unidades Ejecutoras de la Administración Central de suministrar en tiempo y forma la información necesaria para completar los datos de los sistemas informáticos que establezca el Poder Ejecutivo. configurará falta administrativa grave.*"
Por tanto, el responsable de la Base de Datos no es el MIEM, sino que su función se encuadra dentro de una especie de tercero que trata una Base de Datos por una obligación legal. No siendo en consecuencia, responsable de la inscripción de la mencionada Base de Datos.

Pro otro lado, el "Sistema de Gestión Humano (SGH)" a cargo de la Oficina Nacional de Servicio Civil y su normativa regulan un funcionamiento similar.

Asimismo, el "Sistema Integrado de Información Financiera (SIIF)" está a cargo de la Contaduría General de la Nación cuyo objetivo es integrar los distintos componentes de la política fiscal de recursos, gastos y financiamiento, agilizar, mejorar y modernizar la gerencia de los recursos públicos, agilizar substancialmente los procesos de trabajo financieros, mejorar los procesos de toma de decisiones para incrementar la eficiencia en la utilización de los recursos públicos. Dar transparencia a los actos de la administración pública y asignar responsabilidades a los agentes involucrados en el proceso de ejecución de la política fiscal. Este sistema pertenece a Contaduría General de la Nación, por tanto, el MIEM es sólo una especie de encargado de tratamiento.

Conclusiones

Corresponde informar que el MIEM, de acuerdo a la información brindada, es un encargado de tratamiento y por tanto, no es el responsable de la inscripción de aquellas Bases de Datos cuya creación y administración ha sido designada a otros organismos diferentes por diferentes normas.
Que cada Organismo público deberá proceder a la inscripción de sus Bases de Datos dentro del plazo legal establecido, informando que realiza comunicación de datos, bajo qué fundamento legal y determinando los destinatarios.

Es todo cuanto tengo que informar.

Firmado por Dra. Flavia Baladán
Derechos Ciudadanos

Informe N° 157 de 30 de noviembre de 2009.- Se informa sobre una consulta referida a si determinados sujetos regulados por el Banco Central del Uruguay deben registrar sus bases de datos, así como si corresponde documentar el consentimiento de los clientes

Montevideo, 30 de noviembre de 2009

Informe Nº 157/2009
Exp. Nº 2009/084: Consulta sobre el alcance de las bases de datos de las instituciones reguladas por el BCU

- I -

Sobre "Si corresponde que los sujetos regulados por el Banco Central del Uruguay registren sus Bases de Datos" (numeral 1 de la Consulta – fs. 1)

I/A) La consultante transcribe normativa legal y administrativa bancocentralista relativa a "datos mínimos a solicitar" por parte de las instituciones financieras a sus clientes, que hace confluir con lo edictado por los arts. 3C, 24 y 29 (se hace cita errónea al art. 23 cuyo texto es otro) de la Ley Nº 18.331, conduciéndole a sostener una postura exceptuante de las bases de datos así concebidas, respecto del régimen preceptivo en la materia.

Se basa en el art. 34 -que identifica por error como art. 37- de la Carta Orgánica del Banco aprobada por Ley Nº 16.696 de 30-03-1995, con las modificaciones introducidas por la Ley Nº 18.401 de 24-10-2008.

Argumenta que *"los datos que las instituciones deben obtener y conservar, y que por ende forman la Base de Datos de la Institución, son pautados por la normativa bancocentralista, y no datos que la Institución a su arbitrio solicite a sus clientes"*, concluyendo por ello que *"estas Bases de Datos se encuentran totalmente reguladas por una normativa especial, que determina su contenido, quienes deben llevarlas, y el plazo por el cual los datos deben permanecer en la misma"* (fs. 2).

I/B)No se comparte la tesis de la consultante.

En cuanto a la norma orgánica en que se funda, la misma no supone la necesidad de excepcionar las instituciones financieras del régimen general en materia de "protección de datos personales" consagrado por la Ley Nº 18.331 de 11-08-2008.

Y en cuanto a la existencia de una normativa bancocentralista destinada a regular la información que deben suministrar las instituciones financieras, nada impide su armonización con el sistema constitucional y legal de la protección de datos personales.

La postura del informante al respecto es que ni siquiera las bases de datos pertenecientes al BCU (ejemplo la Central de Riesgos Crediticios aludida en la Ley Nº 17.948 de 08-01-2006) escapan al régimen *ut-supra* indicado. Razón *a fortiori* para que tampoco se exceptúen del régimen las bases de datos pertenecientes a las instituciones financieras satelitales del mismo régimen.
I/C) En todo éste tema sobrevuela como cuestión fundamental y previa a cualquier otro entendimiento, la inadvertida necesidad de comprender y aceptar la simbiosis que presentan todos estos regímenes jurídicos (bancocentralista, protección de datos personales, acceso a la información pública), sin tener que desembocar en la fagocitación o excepcionamiento de unos con otros.

El Derecho es uno solo. El correcto entendimiento de las grandes instituciones jurídicas (la protección de datos personales lo es, como también la regulación financiera del país, y desde luego la transparencia del actuar público) comienza por exigir una cuota de naturalidad a efectos de coordinar sus respectivos sistemas jurídicos.

I/D) Es un dato de la realidad que el Banco Central del Uruguay no nació a la vida jurídica con un destino signado o apuntando a la regulación de las bases de datos personales, fenómeno propio de la modernidad más contemporánea insospechado hasta principios de los ´70 del siglo pasado en el mundo europeo, y totalmente ignoto incluso entre nosotros incluso avanzado el nuevo milenio.

Esta realidad apela a nuevas necesidades actuales de control estatal en absoluto conflictivas con la posición constitucional y orgánica que presenta el Banco Central como ente autónomo, lo que determina que los sistemas de información de la Institución y afines (bases de datos tanto del propio BCU como de las entidades reguladas) deban acompasar su régimen jurídico al régimen de protección de datos personales, hoy día contenido fundamentalmente en la doctrina jus-humanista emanante del art. 72 de la Constitución de la República, y en la Ley Nº 18.331.

Es por ello que no procede sostener, como hace la consultante, que las instituciones financieras sometidas a sistemas de contralor bancocentralista están ajenas a cualquier otro dispositivo jurídico que no sea el emanado de la Carta Orgánica del BCU, y de algunas leyes mal llamadas "especiales". De paso se advierte que en nuestro sistema jurídico es en extremo discutible que existan leyes "especiales", e incluso bajo cierto punto de vista, resulta paradojal que sea la propia ley Nº 18.331 la que deba reputarse como "especial" por su materia llegado el caso.
En cualquier caso, asistimos a una premisa equivocada, que es tanto como sostener que las instituciones financieras lo único que tienen para cumplir del régimen legal uruguayo es lo que les ordene o deje de ordenar el Banco Central del Uruguay.

El Banco Central del Uruguay, ciertamente, puede y debe regular a las instituciones financieras. Pero SU regulación no significa que no le quepan al propio Banco, y con mayor razón a las instituciones financieras reguladas por aquél, OTRAS regulaciones jurídicas de diferente tenor. Este segundo grupo de regulaciones, aún adaptadas y

armonizadas, poseen igual título de legitimidad que la normativa bancocentralista, por estar consagradas en el mundo contemporáneo, e incipientemente en nuestro ordenamiento.
I/E) Una de las "instituciones jurídicas" de más rápido y asentado crecimiento en el mundo contemporáneo, es el régimen de protección de datos personales. No se puede negar que la expansión de esta novel rama jurídica en países sin tradición en ella provoca algunas necesidades de ajuste en trámites y operativas que antes no exigían este tipo de miramiento. Pero tampoco es dable, por dicha causa, promover y ejercitar renunciamientos a un régimen que se abre paso firme en la compleja trama social moderna, cuando facilista que privilegian la exclusión del régime. No configura una postura adecuada proceder bajo tal impronta mental. No debe llamar la atención la necesidad de agregar nuevos controles a los existentes, provengan o no del Banco Central. Es lo que sucede, ni más ni menos, con la Ley Nº 18.331, de necesaria y natural aplicación salvo casos muy puntuales y determinados entre los que no revista el pretendido por la consultante.

El régimen en examen, sus particularidades cuando corresponden, deben constituir un acicate intelectual para profundizar y asentar la novel rama jurídica entre nosotros, no siendo aceptable hacerla sucumbir ante la primera dificultad. De lo contrario parecería que se quiere matar la criatura antes de nacer, o en sus cortos primeros años de vida.

Rechazamos con firmeza el intento de crear *ghettos* o compartimentos impolutos a la protección de datos personales dentro del Estado, salvo casos muy contados por especial justificación, entre los que no figuran las bases de datos y sistemas de información del Banco Central del Uruguay. Tal semblante no es correcto del punto de vista jurídico. No se acompasa a la tendencia mundial. Nadie lo está haciendo y a la vista emerge la experiencia española en la materia[45]. En un Estado de Derecho no es admisible que ocurra lo que pretende la consultante, como se verá a continuación.
Citamos del Derecho español[46]: *"La Agencia de Protección de Datos ha resuelto numerosos procedimientos sancionadores por incumplimiento del principio de calidad de datos en el fichero CIRBE* [nota: Central de Información de Riesgos del Banco de España], *tanto por altas improcedentes como por mantener la información inexacta en el mismo. En este mismo sentido, la Audiencia Nacional y el Tribunal Superior de Justicia de Madrid, han dictado sentencias en los recursos contenciosos-administrativos interpuestos por las entidades financieras sancionadas que ratifican las resoluciones impugnadas.*
Así, el Tribunal Superior de Justicia de Madrid, en la Sentencia nº 322, de 21 de marzo de 2001, en el Fundamento de Derecho Tercero señala que «(...) desde el momento en que los

45 La Central de Información de Riesgos del Banco de España se regula por disposiciones normativas de diferente jerarquía, y está sometida al control de la Agencia Española de Protección de Datos como lo demuestran varias resoluciones de ésta, y posteriores fallos judiciales ratificatorios. Por "normativa aplicable" consultar http://www.bde.es/webbde/es/secciones/normativa/be/central_inf_riesgos.html

46 Estudio de la AEPD "La protección de datos en España: análisis y valoración" consultable en https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2002/common/pdfs/D_La-Proteccion-en-Espa-n-a-Valoracion.pdf La cita figura en la pág. 186 del citado Estudio.

datos suministrados al CIRBE por las Entidades de Crédito son accesibles a éstas que pueden recabar la información que precisen para su normal desarrollo (al margen y con independencia del secreto bancario), dicha Central de Información de Riesgos presta, a juicio de esta Sala y Sección además de la función de control, un servicio —aunque limitado a las Entidades de Crédito, por lo que aquí interesa— de Información sobre solvencia Patrimonial y Crédito, y, en tal sentido, la remisión de datos relativos a la solvencia patrimonial de los clientes de las Entidades Bancarias han de cumplir las garantías y requisitos exigidos por el expresado art. 4.1.3, correspondiendo al acreedor —en este caso a la Entidad Bancaria suministradora del dato al CIRBE — la responsabilidad de la veracidad y calidad de los datos suministrados."

Lo que procede es reconocer la realidad, y buscar las requeridas coordinaciones, en vez de anteponer renunciamientos a un régimen constitucional y legal.

El Derecho de la Protección de Datos Personales llegó a estas playas para quedarse, y no para retirarse o retraerse intereses sectoriales mediante por legítimos que éstos sean. No parece inoportuno recordar que se trata de un "derecho inherente a la persona humana", comprendido en el art. 72 de la Constitución de la República (art. 1º de la Ley Nº 18.331), con todas las consecuencias que ello impone a todo nivel, público y privado.

Se trata de un derecho que no agota su explicitación en fórmulas cortas ni meras retóricas. Es un derecho que posee ricos pormenores ontológicos, teóricos y prácticos: requiere reconocimiento, conocimiento y tránsito por parte de los operadores económicos y sociales.

Por "bases de datos creadas y reguladas por leyes especiales" (art. 3 C de la Ley Nº 18.331) sólo procede entender las que cumplen un estándar garantista aunque sea similar -no necesariamente idéntico- al régimen madre, u otro tipo de designios constitucionales que justifiquen su exclusión del régimen. No cabe concebirlo de otra manera, so pena de convertir el dispositivo de la Ley Nº 18.331 (modelado al influjo de un derecho a esta altura del alcance planetario e incluso con vasos comunicantes hacia el entramado internacional) en letra muerta. En tal sentido, la hasta cierto punto muletilla del "excepcionamiento" por vía del art. 3 C de la Ley Nº 18.331 no debe convertirse en fácil válvula de escape a todo un régimen tuitivo de la persona humana (y de las personas jurídicas en lo pertinente), bajo pretexto de la existencia de alguna que otra norma aislada que ni crea, ni regula, ni tiene status de ley especial, reiterando en este último punto la necesidad de esclarecer este concepto, que hoy día no aparece claro al menos en nuestro derecho.

Finalmente, no hesitamos en afirmar que ni la Ley Nº 17.948, ni la Carta Orgánica del BCU trámite Ley Nº 16.696 y su modificativa Ley Nº 18.401, aportan elementos verdaderamente "reguladores" (entendiendo por tales la conformación de un régimen "garantista") al sistema de protección de datos personales. Por esta razón no procede considerar a estas normas como regímenes sustitutivos del consagrado en la Ley Nº

18.331, al que ni siquiera completan y -en el peor de los casos- resultan inaplicables a manos del elemento temporalidad como es el caso de la Ley Nº 17.948 (*lex posteriori derogat lex priori)*, y del elemento especialidad en el caso de la Ley Nº 18.401 (*lex speciali derogat leggi generali)*.

I/F) Se comparte lo sustentado por la consultante.

- II -

Sobre si corresponde "documentar el consentimiento de los clientes" (numeral 2 de la Consulta – fs. 2)

El *principio de consentimiento* cede o se exceptúa en distintas situaciones de expresa consagración legal, e interpretación estricta como corresponde a cualquier excepción legal máxime tratándose de derechos humanos.

Alguna de estas situaciones de excepción se aplican a las actividades que hacen al objeto de la consulta.

El hecho de tratarse de datos recabados "para el ejercicio de funciones propias de los poderes del Estado" y "en virtud de una obligación legal", parecen constituir el fundamento primero y suficiente, para justificar tal exoneración (art. 9 inc tercero B y art. 17 inc. tercero B de la Ley Nº 18.331).

Colaciona al caso, igualmente y en lo pertinente, el hecho de que la hipótesis en examen refiere a informaciones a los que aplica la norma también de excepción "deriven de una relación contractual... del titular de los datos, y sean necesarios para su desarrollo o cumplimiento" (art. 9 inc. tercero D y art. 17 inc. tercero B de la Ley Nº 18.331).

Por todo lo cual resulta admisible prescindir del consentimiento del titular afectado a efectos del registro y tratamiento de sus datos personales. Sin perjuicio de la conveniencia de contar con este consentimiento si no fuera demasiado arduo recabarlo y, de todos modos, la permanencia del deber de informarle siempre al titular sus derechos y obligaciones en la materia (art. 13 de la Ley Nº 18.331).

- III -

Conclusiones

1) La Ley Nº 18.331 de 11 de agosto de 2008 preceptúa y regula el derecho a la protección de datos personales como un derecho inherente a la persona humana comprendido por ello en el artículo 72 de la Constitución de la República (art. 1º de la Ley).

2) La excepción al régimen general, prevista en el literal C) del inciso 3º del artículo 3º de la Ley Nº 18.331, no se aplica a las bases de datos del Banco Central del Uruguay, y *a fortiori* tampoco a quienes meramente aportan in-

formación a dichas bases de datos o constituyen las suyas propias.

3) Ni la Ley Nº 17.948 de 08-01-2006 (información bancocentralista), ni la Ley Nº 16.696 de 30-03-1995, con las modificaciones introducidas por la Ley Nº 18.401 de 24-10-2008 (Carta Orgánica del BCU), aportan elementos verdaderamente "reguladores" en el sentido garantista que exige la correcta interpretación del régimen jurídico en materia de protección de datos personales.

4) Tampoco sucede lo propio -en su caso- con algunas disposiciones administrativas derivadas del ejercicio de la potestad reglamentaria del Ente sobre estos temas, que solamente han tenido presente la facultad supervisora y de control del BCU, pero no el derecho de la protección de datos personales con toda la articulación y pormenores requeridos.

5) En definitiva, a poco que se analizan y repasan este cúmulo de disposiciones, se concluye que resultan insuficientes para enervar el régimen constitucional y legal en materia de protección de datos personales, por cuanto no surge de ellas un manto garantista adecuado al estándar internacional y nacional en esta materia, siendo así inaplicable el excepcionamiento pretendido.

6) Como antecedente ilustrativo de la *opinio juris* imperante en el derecho comparado, que va en sentido contrario al propugnado por la consultante, el fichero CIRBE a cargo del Banco de España (similar al CRC a cargo del BCU), si bien sometido a algunas particularidades normativas (Ley 44/2002 de 22 de noviembre y Circular 31/1995 de 25 de setiembre), de todos modos encarta dentro de la jurisdicción de la Agencia Española de Protección de Datos, debiendo observar las normas de creación, registro y principios generales propios de la materia, so pena de juzgamiento y sanción, incluso en la vía judicial.

7) Respecto de la posibilidad de prescindir del consentimiento de los clientes a la hora de recabar y transmitir este tipo de datos, la respuesta debe ser afirmativa, basada en lo dispuesto por los arts. 9 y 17 de la Ley Nº 18.331 que autoriza tal prescindencia ("ejercicio de funciones propias de los poderes del Estado", "obligación legal", "relación contractual... necesarios para su desarrollo y cumplimiento"), sin perjuicio de mantenerse vigente el deber-derecho de información en favor del titular de los datos conforme el art. 13 de la Ley Nº 18.331.

Firmado por Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 331 de 30 de diciembre de 2009.- Se informa sobre una consulta realizada por Lloyds TSB Bank con respecto a la recolección de consentimiento de clientes anteriores a la Ley N° 18.331y el Decreto N° 414/009

Montevideo, 30 de diciembre de 2009

Informe Nº 331/2009
Exp. Nº 2009/114: Consulta LLOYDS TSB consentimiento clientes anteriores a Ley 18331 y Decreto 414/009

- I -

Se consulta sobre si procede recabar el consentimiento informado de personas físicas y jurídicas clientes de la Institución, cuyos datos obran en poder de ésta con anterioridad a la Ley Nº 18.331 y su decreto reglamentario Nº 414/009.

La propia consultante adelanta opinión negativa sobre el punto, argumentando el principio de no retroactividad de las leyes, y la imposibilidad práctica de obtener el consentimiento escrito y expreso para los datos ya existentes, no así para los nuevos clientes.

- II -

Se comparte parcialmente la postura del consultante por fundamentos diferentes a los que expone la consultante.

La Ley Nº 18.331 de 11 de agosto de 2008 establece que no será necesario el previo consentimiento, entre otros casos, cuando los datos se recaben "en virtud de una obligación legal", o cuando "deriven de una relación contractual" (art. 9 inc. 3 lits. A y D de la ley). Estas y no otras son las hipótesis en juego para el caso planteado, no habiendo más que apelar a ellas para dar respuesta acabada a la consulta.

En cuanto a la primera hipótesis ("obligación legal…"), habrá de tenerse presente que las instituciones bancarias presentes en la plaza conforman el sistema financiero nacional, y están bajo la superintendencia del Banco Central del Uruguay regulada legalmente por su Carta Orgánica, situación de la que emanan una serie de controles naturalmente envolventes del registro y tratamiento de datos personales pertenecientes a los clientes de dichas instituciones (Ley Nº 16.696 de 30-03-1995).

En cuanto a la segunda hipótesis ("relación contractual…"), el vínculo de partes que asumen Banco y cliente determina igualmente la necesidad de que el prime-

ro cuente con determinado número de datos personales del segundo, a efectos de asegurar y desarrollar dicho vínculo.

Ambas razones son suficientes para prescindir de obtener el consentimiento del titular a los efectos del registro y tratamiento de sus datos, dentro de un encuadre de cumplimiento de los restantes principios de la Ley Nº 18.331 (legalidad, finalidad, proporcionalidad, etc.).

- III -

No le asiste razón a la consultante cuando expresa que "con relación a las personas que ya son clientes, nada debemos hacer". Tampoco resulta de recibo su afirmación de que si "dichas personas... en el futuro decidieran desvincularse comercialmente sí podrían ejercer los derechos conferidos por la ley 18.331 y su decreto reglamentario". Se trata de apreciaciones globales o de bloque, que no se compadecen con la letra y espíritu del régimen establecido.

Con respecto a la primera aseveración de la consultante, debe observarse que la prescindencia del consentimiento informado de los clientes actuales no supone que no se aplique el resto del régimen legal en materia de protección de datos personales. Por el contrario la/s bases de datos de clientes ya existentes, igualmente deben registrarse ante la Unidad (arts. 28 y 29 de la Ley), así como respetar los restantes principios y deberes que emanan de la Ley.

Con respecto a la segunda aseveración, no es del caso sostener, como parece hacerlo la consultante, que recién una vez que el cliente se desvincule de la Institución, podrá ejercer los derechos conferidos por el régimen legal, ni tampoco –como ya se expresara en el párrafo anterior- que quepa prescindir de otros deberes de los tomadores de estos datos, consagrados igualmente en la misma ley y que subsisten a pesar del abatimiento del principio del previo consentimiento informado.

Por el contrario, estos clientes ya existentes están plenamente legitimados para ejercer sus derechos (vg. información, acceso…), tanto como están los nuevos. Y habrán de regir a su respecto también, todos los restantes deberes que pone la Ley Nº 18.331 en cabeza de los responsables titulares de las bases de datos en cuestión. Todo ello sin perjuicio de advertir que la figura "cliente" no resulta técnicamente la más apropiada al caso, en la medida que la Ley Nº 18.331 alude a "relación contractual" (art. 9 inc. 3 lit.) y es a este concepto al que habrá de atenerse cualquier interpretación y aplicación del régimen, que deba practicarse sobre el punto.

- IV -
En síntesis

1) La Ley Nº 18.331 establece una serie de derechos en favor de los titulares de

datos personales, consagrados bajo la forma de *principios* de alcance general salvo las excepciones consagradas en la misma Ley con distintos grados de alcance: excepciones al ámbito objetivo de la Ley (art. 3); excepciones al previo consentimiento informado por parte de los titulares de datos personales, para el tratamiento de los mismos (art. 9 inc. 3).

2) Las Instituciones Bancarias pueden prescindir del previo consentimiento informado de sus "clientes" no por el hecho de que éstos ya tuvieran esta calidad a la fecha de entrada en vigencia de la Ley Nº 18.331, ni en base a supuestas "imposibilidades prácticas" para recabarlo, sino con arreglo a los preceptos exceptuantes que emanan de la propia Ley Nº 18.331.

3) Al respecto, existen dos excepciones legales aplicables a la especie y que están contenidas en la Ley Nº 18.331, en el art. 9 inc. 3 lits. B y D. La primera de ellas (literal B: "…obligación legal") se corresponde con el régimen estatuido por la Ley Nº 16.696 (Carta Orgánica del Banco Central del Uruguay), del que derivan una serie de controles estatales que incluyen el tratamiento de cierto número de datos personales de los clientes de dichas Instituciones. La segunda (literal D: "…relación contractual") en tanto y cuanto se trate de datos proporcionados en el marco de un vínculo inter partes que hace necesario tal registro.

4) Por una u otra vía de excepción, en tanto la Institución Bancaria se atenga a los límites y encuadre de las mismas respetando –entre otros- los principios de finalidad y proporcionalidad, podrá prescindirse de obtener el previo consentimiento informado de los "clientes" existentes, entendiéndose por tales aquéllos que conservan una relación contractual a la fecha de entrada en vigencia de la Ley Nº 18.331.

Firmado por Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe sobre interpretación y alcance de la Ley N° 18.331, de 11 de agosto de 2008, de protección de datos personales y acción de habeas data, respecto de los datos personales no incluidos en bases de datos

Montevideo, 19 de noviembre de 2009

Ref. Interpretación y alcance de la Ley Nº 18.331 de 11-08-2008 de protección de datos personales y acción de habeas data respecto de los datos personales no incluidos en bases de datos.

- I -

Para el suscrito no cabe ninguna duda acerca del alcance amplio de la Ley Nº 18.331 de 11-08-2009, cuyo régimen en clave protectora se extiende a los datos personales no necesariamente organizados bajo la forma de base de datos.
El art. 1º de la Ley fundamenta sobradamente esta postura cuando alude al "derecho a la protección de datos personales" como "inherente a la persona humana" y lo hace sin distingos de especie alguna. En ningún texto jurídico se expresa que los datos personales bajo tuición legal, sean exclusivamente aquellos insertos en bases de datos. La Ley lo único que hace es desenvolver un derecho fundamental, de vis constitucional y entendimiento jus-naturalista, por lo que nos encontramos ante un derecho anterior a todo reconocimiento por el derecho positivo, que rige en su máxima extensión, aún sin legislación y/o reglamentación expresas (arts. 72 y 332 de la Constitución de la República), con la sola limitación de las leyes que se dictaren por razones de interés general (art. 7 de la Constitución de la República).
Aún con ser el principal, éste no es el único argumento que fundamenta la postura, sino que existen por lo menos dos argumentos más, claros y precisos, que emanan del articulado de la Ley, a saber:

1) Al establecer el "ámbito objetivo" (art. 3 de la Ley) el legislador no introdujo ninguna limitación en cuanto a que el continente o encuadre de los datos personales debiera ser necesariamente una "base de datos". Se aplica aquí el principio irrefragable de la interpretación jurídica, que señala que "donde el legislador no distingue, no debe hacerlo el intérprete.

2) La letra de la norma no solamente no restringe a texto expreso su ámbito objetivo a los datos que estuvieran contenidos en bases de datos, sino que da un paso más adelante de modo expreso, indicativo en este caso de la clara presencia de una voluntad legislativa no restrictiva. Ello se aprecia cuando el mismo art. 3 de la Ley vincula el registro del dato personal a una conceptualización genérica: "datos personales registrados *en cualquier soporte...*". Si el

legislador hubiese querido circunscribir el ámbito objetivo a los "datos personales registrados *en bases de datos*" (una especie de soporte), jamás hubiera podido hacer la referencia que hizo a "cualquier soporte".

3) Al abordar una serie de definiciones, el legislador incluye la de "dato personal", y nuevamente vuelve a utilizar expresiones indicativas de una amplitud conceptual: "información *de cualquier tipo...*" (art. 4 de la Ley).

- II -

La confusión o duda sobre el tema en examen, pudiera provenir de otra circunstancia de origen igualmente legal que, en todo caso, tiene su explicación y justificación interpretativas, de modo tal que dicha circunstancia no conmueve la postura antes fundamentada. Nos detendremos a continuación en este punto, a efectos de explicarlo con precisión.
El factor que puede llamar a confusión es que el legislador utiliza la expresión "bases de datos" en varios pasajes de la ley Nº 18.331. Y es que no son pocas las veces que lo hace. Son treinta (30) coincidencias, algunas de las cuales -por vía de ejemplo- se analizan a continuación con su correspondiente argumento o explicación de por qué no conmueven la tesis defendida en el presente Informe:

1) Art. 3: "No será de aplicación a las siguientes bases de datos". Explicación – Refiere a excepciones, por lo que no vulnera la regla. Nada impide que el legislador siente la regla general referida a los datos personales y a su protección dentro de cualquier contexto de entendimiento (dentro o fuera de bases de datos), y a la hora de prever excepciones -como lo hace- refiera las mismas exclusivamente a situaciones donde los datos personales integran bases de datos.

2) Art. 3: "C) A las bases de datos creadas y reguladas por leyes especiales". Explicación - Idem 1.

3) Art. 4: "I) Fuentes accesibles al público: aquellas bases de datos cuya consulta..." Explicación - Si no fuera que se trata de un argumento bastante lateral, podría llegar a conmover la tesis asumida en el presente Informe. El legislador no debió vincular el concepto de "fuentes públicas de información" al de "bases de datos" como lo hace en este artículo, aún bajo la concepción amplia (y no totalmente coincidente con la propia de la Informática), que utiliza la ley al referir a las bases de datos (art. 4A de la Ley). En estricta lógica son tan "fuentes públicas..." las que se originan o provienen de una base de datos, como las que consisten o emanan de datos personales aislados. Esto es así al punto que el art. 9 inc. 3 literal A de la Ley establece como una de las excepciones al previo consentimiento "los datos que provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación", expresiones o ejemplos que nada o poco tienen que ver necesariamente con "bases de datos" (cuanto menos el segundo).

4) Art. 5: "La actuación de los responsables de las bases de datos...". Explicación – El mismo texto amplía el elenco de sujetos a "en general, de todos quienes actúen en relación a datos personales de terceros...", con lo cual desaparece el argumento pro bases de datos.

5) Art. 6: "La formación de bases de datos será lícita..." Explicación – Es totalmente congruente. Los datos personales considerados en sí mismos no son lícitos ni dejan de serlo. La calificación va al registro y tratamiento que se haga de ellos, actividades que -por fuerza- refieren a las bases de datos, no a los datos en sí.

6) Las restantes menciones del texto legal a "bases de datos" no implican desaplicar el régimen en lo pertinente con respecto a aquellos datos personales que se encuentran fuera de ellas. Se haría por demás extenso continuar con las citas y explicaciones respectivas, por lo que sin pretender una exhaustividad valdrán como argumentaciones finales las siguientes:

   • De todas estas menciones surge la conclusión de que la ley se preocupa prioritariamente por las bases de datos, conformando un verdadero régimen jurídico en su torno: registro; conductas debidas, facultativas o prohibidas, casos especiales.
   • Existe un fundamento lógico y racional para ello, en cuanto a que las acciones potencialmente más peligrosas (en términos cualitativos y cuantitativos) se originan a partir de este tipo de soportes o formas organizativas de la información, no así en cuanto a un uso aislado de los datos personales.
   • Pero ello no significa que la regulación resulte excluyente. Se trata de razones de preferencia pero no de exclusividad. Sin duda aparece plausible la existencia de un régimen jurídico orgánico y articulado en referencia a las bases de datos, pero ello no implica dejar de lado su aplicación -en lo pertinente- a los datos personales individualmente considerados.

- III -

El derecho comparado muestra igual impronta que la sustentada en el presente Informe. El concepto de "dato de carácter personal" se define en el artículo 3.a) de la LOPD española como *"Cualquier información concerniente a personas físicas identificadas o identificables",* y en el artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la disposición transitoria tercera de la LOPD, se define como *"toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable"*.
En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE, del Parlamento y del Consejo, de 24/10/1995, relativa a la protección de las perso-

nas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. La Directiva europea aporta un concepto lato de "dato personal", entendiendo por tal *"toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*. Asimismo, el Considerando 26 de la citada Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable.

El Grupo de Trabajo del Art. 29 se pronuncia con total precisión y claridad al respecto, adoptando la tesis amplia: *"... para que la información sea considerada como datos personales no es necesario que esté recogida en una base de datos o en un fichero estructurado. También la información contenida en un texto libre en un documento electrónico puede calificarse como datos personales, siempre que se cumplan los otros criterios de la definición de datos personales. El correo electrónico, por ejemplo, contiene datos personales".* (Dictamen Nº 4/2007 sobre el concepto de datos personales – WP 136).

- IV -
Conclusiones

Existen varios argumentos por los cuales se concluye que los datos personales no incluidos en bases de datos están igualmente alcanzados por la Ley Nº 18.331.

El fundamento principal de tal conclusión es que el legislador no hace distingos a la hora de caracterizar y delinear el régimen, y es así que el "derecho a la protección de datos personales" es un derecho inherente a la persona humana afincado en los arts. 72 y 332 de la Constitución de la República, con la sola limitación que pudiera emerger de las leyes dictadas por razones de interés general, conforme art. 7 de la misma Carta.

Como argumentos complementarios en la misma dirección antes apuntada, se aprecia que al definirse el "ámbito objetivo" de la Ley Nº 18.331 en su art. 3, tampoco se introdujo limitación o encuadre con respecto del continente que debieran observar los datos personales, y por el contrario se introdujo una conceptualización expresamente genérica al respecto, al aludirse a "datos personales registrados en cualquier soporte".

No es del caso dejarse obnubilar por las nutridas referencias a "bases de datos" que contiene la Ley, para sentirse obligado a sostener que la misma regula las bases de datos en vez de algo mucho más trascendente como es el "derecho a la protección de los datos personales", estén donde estén estos últimos. Esta cir-

cunstancia es fruto desde luego de la preocupación y regulación específicas por este tipo de soportes con relación al derecho en juego, ya que es en su entorno donde radican los mayores riesgos y aconteceres relativos al derecho regulado. Pero el punto no inhibe la necesidad jurídica de considerar y preservar a éste derecho (que siempre es el mismo como derecho) en todas sus otras expresiones, aún aquéllas que no condigan o se relacionen con bases de datos.
El derecho comparado consultado apoya la tesis amplia sustentada, según surge de la normativa y doctrina explicitadas en el cuerpo del Informe (LOPD española, considerando 26 y art. 2a de la Directiva 95/46/CE, WP136 correspondiente al Dictamen Nº 4/2007 del Grupo de Trabajo del Art. 29).

Firmado por Dr. Marcelo Bauzá
Derechos Ciudadanos

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

Andes 1365 piso 8, Montevideo, Uruguay Tel.: (+598) 2901 2929 ext. 1352
Email: info@datospersonales.gub.uy
www.datospersonales.gub.uy