2011

RESOLUCIONES
DICTÁMENES E INFORMES

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

Índice

Contenido

Resolución N° 39 de 4 de febrero de 2011.
Se resuelve sobre la utilización de datos personales sin consentimiento de la denunciante.

RESOLUCION N°		EXPEDIENTE N°
39	2011	2377/2011

Montevideo, 4 de febrero de 2011.

VISTO:

La denuncia presentada por utilización de datos personales sin consentimiento de la denunciante titular afectada.

RESULTANDO:

I.- Que se trató de la comunicación de un número telefónico por parte de AA S.A. a BB, y que un empleado de ésta (mensajero) utilizó un día domingo en horas de la mañana, para posibilitar la entrega de la tarjeta de crédito emitida por la primeramente nombrada en favor de la denunciante.

II.- Que el expediente se instruyó escuchando las alegaciones de todos los interesados, denunciante y denunciadas.

III.- Que la denunciada AA S.A. aportó finalmente el número telefónico en un documento de tipo vinculante por estar firmado por la denunciante, si bien de fecha posterior al contrato principal donde figuraban sus restantes datos.

CONSIDERANDO:

I.- Que esta ulterior probanza es determinante para concluir que los hechos denunciados e investigados no revelan infracción a la Ley Nº 18.331.

II.- Que sin perjuicio de ello, la denuncia y actuaciones cumplidas en su mérito, han dejado al descubierto la inadecuación documental y práctica de las denunciadas, especialmente de AA S.A., al régimen legal y reglamentario de la protección de datos personales que rige en el país.

III.- Que en efecto, el modelo de contrato de AA S.A. para emisión y entrega de tarjetas de crédito, no contiene cláusula alguna relativa al régimen tutelar objeto de control.

IV.- Que el documento contractual principal fue otorgado durante la vigencia de la anterior Ley Nº 17.838, que no contenía la preceptiva orgánica y completa de la actual, en tanto el documento posterior en el que figura el número telefónico lo fue durante la vigencia del plazo de adecuación de la actual Ley Nº 18.331.

V.- Que en cambio parece oportuno y necesario exigir a ambas empresas que dispongan de ahora en adelante lo pertinente para cumplir el régimen proteccionista de mejor grado a como lo han venido haciendo.

VI.- Que a tales efectos se recomendará a ambas empresas que, en plazo prudencial, ajusten los documentos

contractuales y prácticas empresariales en los cuales tratan con datos personales, en orden a asegurar el cumplimiento de los principios de legalidad, veracidad, finalidad, seguridad, reserva y responsabilidad, así como la vigencia efectiva de los derechos de información frente a la recolección de datos, de acceso, rectificación, actualización, inclusión o supresión, impugnación de valoraciones personales y comunicación de datos. Se evitará tratar datos sensibles salvo especial justificación, y se cumplirán en lo pertinente las previsiones especiales contenidas en los arts. 21 y 22 de la Ley Nº 18.331.

ATENTO:

A lo expuesto y lo dispuesto por el artículo 72 de la Constitución de la República, y los artículos 5° a 17, 21 y 22 de la Ley N° 18.331, concordantes y afines.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

I) DECLARAR QUE NO HUBO INFRACCIÓN EN LOS HECHOS DENUNCIADOS, Y POR ENDE NO SANCIONAR A AA S.A. Y BB, SIN PERJUICIO DE ESTIMAR QUE DEBEN PRESTAR MAYOR ATENCIÓN EN EL DESARROLLO DE SUS ACTIVIDADES, AL RÉGIMEN LEGAL Y REGLAMENTARIO DE PROTECCIÓN DE DATOS PERSONALES VIGENTE EN EL PAÍS.

II) EN CONSECUENCIA, RECOMENDAR A AMBAS EMPRESAS QUE REVEAN EN LO PERTINENTE LOS DOCUMENTOS Y PRÁCTICAS EMPRESARIALES DONDE TRATAN DATOS PERSONALES, AJUSTÁNDOSE A LAS DISPOSICIONES VIGENTES EN LA MATERIA, DANDO CUENTA POSTERIORMENTE DE LO ACTUADO EN ESTE SENTIDO.

III) NOTIFÍQUESE A TODOS LOS INTERESADOS Y CLAUSÚRENSE LAS ACTUACIONES SIN PERJUICIO DE MANTENER LAS MISMAS A DESPACHO, EN VIRTUD DE LO ESTABLECIDO EN EL NUMERAL PRECEDENTE. PUBLÍQUESE.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo
URCDP

m.b.

Resolución N° 320 de 17 de marzo de 2011.
Se adecuan las sanciones administrativas en virtud de las modificaciones introducidas por la Ley N° 18.719, de 27 de diciembre de 2010.

RESOLUCION N°		EXPEDIENTE N°
320	2011	47/2011

Montevideo, 17 de marzo de 2011.

VISTO:

La necesidad de adecuar las sanciones administrativas, en virtud de las modificaciones introducidas por la Ley N° 18.719, de Presupuesto Nacional.

RESULTANDO:

Que el 16 de julio de 2010 se dictó la Resolución N° 890/2010 sobre graduación de sanciones administrativas, la que debe ser modificada a la luz de los cambios verificados.

CONSIDERANDO:

I) Que el artículo 152 de Ley N° 18.719 modifica el artículo 35 de la Ley de Protección de Datos Personales y Acción de Habeas Data N° 18.331 (LPDP), estableciendo que el Órgano de Control podrá aplicar a los responsables de las bases de datos, encargados de tratamiento de datos personales y demás sujetos alcanzados por el régimen legal que infrinjan las disposiciones de la LPDP, las siguientes sanciones:
Observación.
Apercibimiento.
Multa de hasta 500.000 UI (quinientas mil unidades indexadas).
Suspensión de la base de datos respectiva por el plazo de cinco días.
Clausura de la base de datos respectiva.

II) En la tarea de graduación, se contemplará que la infracción cometida encuadre en la categoría de muy leve, leve, grave o muy grave.

III) Se calificarán como infracciones muy leves, sin que ello signifique una enumeración taxativa:
Haber presentado la solicitud de inscripción de la base de datos, sin haber culminado el trámite por razones que atañen al solicitante.
Incumplir el derecho de opción que tiene el titular de los datos acerca del medio por el cual desea le sea suministrada la información (escrito, medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin), conforme lo dispuesto en el artículo 14 inciso 6° de la LPDP.

IV) Se calificarán como infracciones leves, sin que ello signifique una enumeración taxativa:

1. No haberse presentado a inscribir la base de datos respectiva.

2. Recolectar datos personales de los titulares, sin cumplir con el deber de informar que prevé el artículo 13 de la LPDP.

3. No atender por razones formales a las solicitudes de los titulares de los datos cuando comparezcan a ejercer alguno de los derechos consagrados en la LPDP.

4. Incumplir el deber de secreto establecido en el artículo 11 de la LPDP, siempre que no constituya infracción grave.

5. No brindar a la URCDP la información que ésta le solicita, en el marco de las competencias atribuidas por Ley.

V) Se calificarán como infracciones graves, sin que ello signifique una enumeración taxativa:

1. Crear Bases de Datos de titularidad pública o iniciar la recolección de datos personales sin el consentimiento del titular de los datos, fuera de las hipótesis contempladas en los literales B) y D) del artículo 9° de la LPDP.

2. Crear Bases de Datos de titularidad privada o iniciar la recolección de datos personales, para finalidades distintas o incompatibles de las que constituyen el objeto legítimo de la persona física o jurídica correspondiente.

3. Recolectar datos personales de los titulares sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible, conforme lo dispuesto en el artículo 9° de la LPDP.

4. No inscribir la Base de Datos en el Registro de la URCDP, cuando ello le haya sido requerido por resolución del Consejo Ejecutivo de la Unidad.

5. Tratar o usar datos personales, vulnerando los principios, derechos y garantías consagradas en la LPDP y su reglamentación, cuando no constituya infracción muy grave.

6. Impedir u obstaculizar el ejercicio de los derechos de acceso, rectificación, actualización o supresión que fuere solicitado por el titular de los datos personales.

7. Impedir u obstruir el ejercicio de la actividad inspectiva, prevista por el artículo 34, literal D) de la LPDP y su reglamentación.

8. Mantener los datos personales inexactos o desactualizados o no efectuar las rectificaciones o eliminaciones correspondientes, cuando legalmente proceda, vulnerando los derechos que la LPDP consagra.

9. Violar el deber de secreto sobre los datos personales incluidos en Bases de Datos que contengan datos relativos a comisión de infracciones administrativas o penales, de naturaleza tributaria, servicios financieros, relativos a la actividad comercial o crediticia, así como aquellas otras Bases de Datos que contengan un conjunto de datos personales suficientes para obtener una evaluación de la personalidad del individuo.

10. Mantener las Bases de Datos, locales, equipos o programas que contengan datos personales sin las

condiciones necesarias para garantizar su seguridad y confidencialidad.

11. No remitir a la URCDP, en plazo que ésta fije, los documentos e informaciones que le sean requeridos.

12. Incumplir el deber de informar que prevén los artículos 9° y 13 de la LPDP, cuando los datos personales hayan sido recabados por persona distinta del afectado.

VI) Se calificarán como infracciones muy graves, sin que ello signifique una enumeración taxativa:

1. Recolectar datos personales en forma engañosa y fraudulenta.

2. Comunicar o ceder datos personales, fuera de los casos contemplados en la LPDP.

3. Tratar los datos personales, violentando los principios y garantías consagradas en la LPDP, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

4. Recolectar y tratar datos sensibles, sin el consentimiento expreso y escrito del titular de los datos, conforme lo previsto en el artículo 18 de la LPDP.

5. Recolectar y tratar datos relativos a la salud, fuera de las hipótesis contempladas en el artículo 19 de la LPDP.

6. No cesar el tratamiento y uso ilegítimo de datos personales, cuando le haya sido requerido por los titulares de los datos, o por resolución del Consejo Ejecutivo de la Unidad.

7. La transferencia internacional de datos personales a países que no proporcionen un nivel de protección adecuado, conforme lo dispuesto en el artículo 23 de la LPDP y la Resolución del Consejo Ejecutivo N° 17, de 12 de junio de 2009.

8. La violación al deber de guardar secreto sobre los datos personales sensibles y relativos a la salud, contemplados en los artículos 18 y 19 de la LPDP, sin consentimiento de las personas afectadas.

9. No atender o impedir de forma reiterada el ejercicio de los derechos de acceso, rectificación, actualización, inclusión o supresión.

10. No cumplir de forma reiterada con el deber de información de la inclusión de datos personales en una Base de Datos.

VII) Las sanciones se graduarán, en cada una de las categorías, por tres escalas: Mínimo, Medio y Máximo, apreciándose las circunstancias atenuantes o agravantes que puedan confluir en cada caso, teniendo en cuenta los siguientes guarismos:

Leves: Mínimo de 100 a 3.000 Unidades Indexadas
Medio de 3001 a 6.000 Unidades Indexadas
Máximo de 6001 a 12.000 Unidades Indexadas

Graves: Mínimo de 12.001 a 30.000 Unidades Indexadas
Medio de 31.001 a 60.000 Unidades Indexadas
Máximo de 60.001 a 90.000 Unidades Indexadas

Muy Graves: Mínimo de 90.001 a 150.000 Unidades Indexadas
Medio de 150.001 a 300.000 Unidades Indexadas
Máximo de 300.001 a 500.000 Unidades Indexadas

VIII) En todo caso, para determinar qué sanción es razonable y proporcional al hecho cometido, se atenderá a la gravedad, reiteración o reincidencia de la infracción cometida.
Asimismo, se apreciará el tipo de datos personales objeto de tratamiento, las medidas de seguridad, los derechos personales vulnerados, el volumen de los tratamientos efectuados, los beneficios obtenidos, sean económicos o de otra índole, el grado de intencionalidad, los daños y perjuicios causados a las personas interesadas y a terceras personas, y cualquier otra circunstancia que sea relevante para evaluar la conducta infraccional cometida. También deberán tenerse en cuenta eventuales eximentes de responsabilidad que puedan conjugarse, como la fuerza mayor o caso fortuito.

ATENTO:
A lo expuesto, a lo previsto en las normas citadas y a las facultades conferidas por el artículo 35 de la Ley N° 18.331 (LPDP) en su nueva redacción,
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1) Las sanciones se graduarán como muy leves, leves, graves y muy graves, atendiendo a los parámetros establecidos en los Considerandos.

2) La sanción de observación corresponderá cuando la infracción a las disposiciones de la LPDP sea de carácter muy leve.

3) Se aplicará la sanción de apercibimiento cuando la infracción a las disposiciones de la LPDP sea de carácter leve y no existan antecedentes de infracciones anteriores.

4) Para la imposición de la sanción de multa se tendrá en cuenta si el grado de la conducta infraccional encuadra en la categoría de leve con antecedentes, grave o muy grave.

5) Las sanciones de suspensión o clausura de la base de datos respectiva se impondrán cuando la infracción a las disposiciones de la LPDP sea de carácter muy grave y, en aplicación de los principios de razonabilidad y proporcionalidad, la sanción de multa no resulte lo suficientemente adecuada, atendiendo a la violación de las disposiciones de la Ley.

6) Publíquese en la página web de la Unidad Reguladora y de Control de Datos Personales, y archívese.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo
URCDP

m.j.r.

Resolución N° 720 de 14 de abril de 2011.

Se resuelve denuncia derivada de aportar información errónea respecto al incumplimiento de una deuda.

RESOLUCION N°		EXPEDIENTE N°
720	2011	3030/2011

Montevideo, 14 de abril de 2011.

VISTO:

La denuncia formulada por el Sr. AA (en adelante el denunciante) contra BB (en adelante la denunciada) por haber aportado información errónea en virtud de no haber asentado las cancelaciones de las deudas de que era titular.

RESULTANDO:

I.- El denunciante afirma que en garantía del cumplimiento de un préstamo con la denunciada, constituyó derecho de prenda a favor de ésta, respecto de los certificados de depósitos de su propiedad, por un monto de U$S 12.126,29 y que en procura de su cancelación, autorizó a la entidad bancaria a que éste compensara los importes de las cuotas con el producido del certificado de depósito.
Añade que frente a cada vencimiento, su madre concurría a la entidad bancaria denunciada a depositar en efectivo y por ventanilla, el importe correspondiente a la diferencia entre el monto compensado y el valor de la cuota devengada (escasos dólares de diferencia entre el crédito y el débito), tal como surge de la documentación que incorpora (fs. 18-47).

Concluye que a la fecha prevista para la cancelación de la deuda, en el mes de junio de 09, las partes nada debían a la institución bancaria, no obstante lo cual su categoría crediticia y la de sus padres, ante el Banco Central del Uruguay (BCU), era calificada con la categoría 5, es decir, deudor irrecuperable, incobrable, pese a todos sus reclamos.

II.- Se le otorgó vista a la denunciada, quien manifestó que en virtud del descalce que existía entre lo efectivamente percibido por el Banco en virtud de la prenda sobre certificados y la obligación mensual de pago de lo adeudado, el denunciante mantuvo una diferencia de U$S 48.94, a fin de poder cancelar totalmente el adeudo. Agrega que tal saldo deudor, conforme la normativa vigente del BCU debió ser informado por la denunciada a la entidad reguladora, generándose en consecuencia el correspondiente registro negativo del deudor en dicha base.

III.- Por informe N° 4900/2010 de 16 de diciembre de 2010 se le solicitó a la denunciada que proporcione información acerca de cómo se generó la diferencia de U$S 48.94 y en su caso acredite la notificación de la deuda al denunciante; así como que se aclaren los motivos que ameritaron la comunicación a Clearing de Informes, con fecha 30/06/09, de una operación incumplida a cargo del denunciante, por el monto de US$ 570.

Notificada la denunciada con fecha 23 de diciembre de 2010, no brindó la información requerida.

IV.- Se expidió el informe jurídico N° 4101 de 10 de marzo de 2011, el que luce agregado a fs. 88-90.

CONSIDERANDO:

I.- Que la denunciada infringió el artículo 7° de la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP) que regula el principio de veracidad de los datos, en tanto comunicó al BCU una deuda del denunciante que había sido cancelada en el mes de junio de 2009, violentando la exactitud y actualidad que debe regir en el tratamiento de los datos personales.
Dicho extremo, además de surgir de los recibos aportados por el denunciante a fs. 18-47, no fue controvertido por el denunciado con la documentación acreditante correspondiente.

II.- Que a la conducta infraccional referida se suma la omisión de proporcionar la información que le solicitara el Órgano de Control por informe N° 4900/2010 (fs. 78), contraviniendo lo previsto en el artículo 34 literal E) de la LPDP.

III.- Que la Unidad Reguladora y de Control de Datos Personales (URCDP), conforme las potestades conferidas por el artículo 35 de la LPDP podrá aplicar medidas sancionatorias a los responsables de las bases de datos o encargados del tratamiento de datos personales, cuando violen las disposiciones de la ley.

IV.- Que en el caso, si bien la conducta revestiría gravedad, se impondrá la sanción de apercibimiento, atendiendo a que la denunciada no posee antecedentes de infracciones anteriores.

ATENTO:

A lo expuesto, y a lo previsto en los artículos 7°, 35 y demás disposiciones de la Ley N° 18.331 y su Decreto reglamentario N° 414/009, de 31 de agosto de 2009,
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1) Impóngase a Nuevo Banco Comercial, la sanción de apercibimiento.
2) Notifíquese y oportunamente, publíquese.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo
URCDP

m.j.r.

Resolución N° 858 de 26 de mayo de 2011.

Se resuelve sancionar a una empresa por el envío de correo electrónico no deseado.

RESOLUCION N°		EXPEDIENTE N°
858	2011	57/2011

Montevideo, 26 de mayo de 2011.

VISTO:

La denuncia presentada por envío de correo no solicitado.

RESULTANDO:

I.- Que se dio trámite a la misma, dando oportunidad a la denunciada para que formulara sus descargos.

II.- Que en comparecencia a fs. 9 la denunciada sostiene que se trató de un correo electrónico enviado como favor por un amigo de la familia, a quien le solicitó hacer este envío tan solo a su clientela pero el mismo terminó ampliado a una lista de contactos del gestor.

CONSIDERANDO:

I.- Que las explicaciones ofrecidas no satisfacen ni alcanzan para desmentir la infracción cometida, encontrándonos ante un caso de lo que en doctrina se denomina “spam”, vale decir comunicación no solicitada realizada por vía electrónica.

II.- Que la hipótesis así encuadrada configura un incumplimiento del art. 21 de la Ley Nº 18.331 en su actual redacción dada por el art. 152 de la Ley Nº 18.719, ya que el correo de la denunciante es un dato personal, y el mismo no fue tomado de un documento accesible al público, ni facilitado por su titular, ni obtenido con su consentimiento.

III.- Que consta, asimismo, que la denunciada no ha inscripto su/s base/s de datos/s personales ante esta Unidad, conforme ordenan los arts. 28 y 29 de la Ley Nº 18.331 en sus respectivas redacciones actuales dadas respectivamente por los arts. 152 y 154 de la Ley Nº 18.719.

IV.- Que atendiendo la primariedad de los ilícitos cometidos, corresponde aplicar la sanción mínima dentro de la escala legalmente vigente, e intimar la inscripción antes mencionada.

ATENTO:

A lo expuesto, al Informe Letrado agregado a fs. 10, y a lo dispuesto por los artículos 1°, 4° D), 21, 28, 29 y 35 1) de la Ley N° 18.331 y su modificativa Ley Nº 18.719,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

I) SANCIONAR CON "OBSERVACIÓN" A LA EMPRESA MARÍA NOELIA PEREYRA CARBONI QUE GIRA BAJO EL NOMBRE DE FANTASÍA "MARÍA BONITA" POR INFRACCIÓN A LA LEY Nº 18.331 (ENVÍO DE CORREOS NO SOLICITADOS).

II) INTIMAR A LA MISMA EMPRESA EL REGISTRO DE LA/S BASE/S DE DATO/S PERSONALES QUE DISPONGA, EN EL PLAZO DE TREINTA DÍAS CORRIDOS BAJO APERCIBIMIENTO DE MAYORES SANCIONES SI NO LO HICIERE.

III) NOTIFÍQUESE Y PUBLÍQUESE.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo
URCDP

m.b.

Resolución N° 945 de 29 de junio de 2011.

Se aprueban artículos destinados a integrarse en la norma reguladora del Sistema Integrado de Información en el Área Social (SIIAS) del Ministerio de Desarrollo Social.

RESOLUCION N°		ACTA
945	2011	21/2011

Montevideo, 29 de junio de 2011.

VISTO:

Las reuniones mantenidas con los responsables del Sistema Integrado de Información en el Área Social, dependiente del Ministerio de Desarrollo Social, del que surgiera la consulta sobre su adecuación al régimen legal de protección de datos personales.

RESULTANDO:

Que se realizó el estudio respectivo, del cual emergió un proyecto normativo de cuatro artículos, a integrarse en la norma reguladora del Sistema en su conjunto.

CONSIDERANDO:

I.- Que entre las competencias de la Unidad figuran la de asistir y asesorar a las personas que lo requieran acerca de los alcances de la ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.

II.- Que a la Unidad le compete también la emisión de opinión toda vez que le sea requerida por las autoridades competentes.

ATENTO:

A lo expuesto, a lo que surge del art. 621 de la Ley Nº 18.719 de 27 de diciembre de 2010, y del art. 34 lits. A) y F) de la Ley N° 18.331. El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

I) APROBAR CUATRO ARTÍCULOS DESTINADOS A SUGERIR LA REGULACIÓN DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES DEL SISTEMA INTEGRADO DE INFORMACIÓN EN EL ÁREA SOCIAL, DEL MINISTERIO DE DESARROLLO SOCIAL.

II) COMUNICAR EL TEXTO APROBADO AL ORGANISMO CONSULTANTE, EL QUE FIGURA EN ANEXO ÚNICO A LA PRESENTE RESOLUCIÓN.

Fdo: Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

ANEXO ÚNICO

CAPÍTULO…

Protección de Datos Personales

Artículo 1º. El SIIAS maneja información de personas y prestaciones que se consolidan a partir de las bases de datos de los organismos integrados al sistema, a saber:

I) Administración de los Servicios de Salud del Estado (ASSE),

II) Banco de Previsión Social (BPS),

III) Instituto del Niño y Adolescente del Uruguay (INAU),

IV) Ministerio de Desarrollo Social (MIDES),

V) Ministerio de Salud Pública (MSP),

VI) Otros que se incorporen cuando se encuentren con la necesaria capacidad de integración de datos.

Los organismos intervinientes deberán formalizar su adhesión al acuerdo en el que se establezca los mecanismos, condiciones de intercambio de datos, y demás requisitos conforme lo dispuesta por los artículos 157 a 160 de la Ley Nº 18.719 de 27 de diciembre de 2010.

Artículo 2º. Los organismos que integren el sistema comunicarán los datos que fueren necesarios para el cumplimiento de los fines relacionados con intereses legítimos del emisor y del destinatario en ejercicio de sus respectivas competencias.

Artículo 3º. Toda vez que el funcionamiento del SIIAS requiera el tratamiento de datos personales no disociado de sus titulares, se deberán cumplir con los principios de legalidad, veracidad, finalidad, seguridad, reserva y responsabilidad definidos en el Capítulo II de la Ley Nº 18.331, de 11 de agosto de 2009, de Protección de Datos y Acción de Habeas Data (LPDP).

La comunicación de los datos personales al SIIAS no requerirá el consentimiento de sus titulares, aún tratándose de datos sensibles (artículos 17 inciso 3º apartado A) y 18 de la LPDP, y artículo 621 de la Ley Nº 18.719 de 27 de diciembre de 2011).

Artículo 4º. El titular de los datos personales gozará de los derechos de acceso, rectificación, actualización, inclusión o supresión, e impugnación de valoraciones personales, de acuerdo con lo establecido en el Capítulo III de la LPDP.

El SIIAS (Ministerio...) coordinará la adopción de las medidas organizativas y tecnológicas que garanticen el ejercicio efectivo de sus derechos a los titulares.

Resolución N° 990 de 8 de julio de 2011.

Se resuelve sancionar a una empresa por denuncia motivada en el envío de correo electrónico no deseado.

RESOLUCION N°		EXPEDIENTE N°
990	2011	036/2011

Montevideo, 8 de julio de 2011.

VISTO:

La denuncia presentada por envío de correos electrónicos no solicitados (spam).

RESULTANDO:

I.- Que se sustanció la misma con vista al denunciado a fin de que presentara sus descargos.

II.- Que al evacuar la vista conferida a fs. 21, el denunciado reconoció como forma habitual de divulgar sus cursos el envío de correos electrónicos. Explica que los mismos se encuentran contenidos en dos bases de datos de las cuales es responsable. Manifiesta asimismo, que sus comunicaciones cuentan con la opción para que el destinatario pueda darse de baja. Por último, expresa que no puede responder en qué base de datos se encuentra la denunciante por la reserva de su identidad.

III.- Que debido a la referida reserva, se confirió vista a la denunciante de lo manifestado por el denunciado solicitándole autorización para revelar su correo electrónico. La denunciante denegó la autorización pedida.

CONSIDERANDO:

I.- Que si bien la denunciante no autorizó la revelación de su correo electrónico y respecto de la misma no es posible determinar si se configuró el envío de comunicaciones electrónicas no solicitadas por el denunciado, de los descargos presentados se desprenden irregularidades que fundamentan la prosecución de estas actuaciones, las que se mencionan a continuación.

II.- Que las bases de datos responsabilidad del denunciado no se encuentran inscriptas ante esta Unidad lo que configura incumplimiento a la Ley N° 18.331.

III.- Que de los descargos presentados se advierte la existencia de más bases de datos que las declaradas.

IV.- Que el denunciado no ha probado en las presentes actuaciones que los titulares de los correos electrónicos que admite utilizar, hubiesen consentido el tratamiento a fin de recibir ofertas sobre los cursos que imparte.

V.- Que considerando la primariedad, corresponde la aplicación de una observación al denunciado, intimándosele conjuntamente al registro de todas las bases de datos de las que sea responsable en el plazo 30 días corridos.

ATENTO:

A lo expuesto, y al informe agregado a fs. 40, en función de lo preceptuado en los artículos 6°, 9° y 35 de la Ley N° 18.331, este último en su redacción dada por el artículo 152 de la Ley N° 18.719,
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

I) OBSERVAR A RENGLÓN UNO – CAPACITACIÓN EMPRESARIAL LTDA. POR INFRACCIÓN A LA LEY Nº 18.331 AL INCUMPLIR CON EL REGISTRO DE LAS BASES DE DATOS DE LAS CUALES ES RESPONSABLE Y TRATAR EL DATO PERSONAL CORREO ELECTRÓNICO SIN CONSENTIMIENTO DE SUS TITULARES PARA ENVIAR CORREOS ELECTRÓNICOS NO SOLICITADOS.

II) INTIMAR A LA REFERIDA EMPRESA A REALIZAR EL REGISTRO DE TODAS SUS BASES DE DATOS PERSONALES EN EL PLAZO DE TREINTA DÍAS CORRIDOS.

III) NOTIFÍQUESE Y PUBLÍQUESE.

Fdo. Mag. Federico Monteverde.
Consejo Ejecutivo
URCDP

b.m.

Resolución N° 1030 de 20 de julio de 2011.

Se resuelve sancionar a una empresa por envío de correo electrónico no deseado.

RESOLUCION N°		EXPEDIENTE N°
1030	2011	38/2011

Montevideo, 20 de julio de 2011.

VISTO:

La denuncia presentada contra AA Sucursal Uruguay por envío de spam a su casilla de correo electrónico institucional.

RESULTANDO:

I.- Que la denunciante presenta copia de los correos electrónicos enviados en dos oportunidades, con información promocional de la empresa, referida a sorteos y términos y condiciones de los mismos.

II.- Que es relevante indicar que el correo electrónico de la denunciante es institucional, -proporcionado por el organismo público para el cual trabaja-, y que dicha dirección electrónica contiene precisamente el nombre y apellido de la denunciante, así como su lugar de trabajo, lo cual permite identificarla plenamente.

III.- Que en sus descargos, AA afirma que la única forma en que una persona puede recibir información de la empresa, es si previamente se ha inscripto en la web y lo ha consentido. Que en este caso, fue justamente mediante el llenado de un formulario durante un evento organizado por la empresa, que los datos de la denunciante fueron ingresados al listado, pero dada la gran cantidad de volumen de documentación que la empresa maneja dicho formulario fue destruido pasado un tiempo razonable, siendo por eso que no cuentan con dicho documento para poder aportarlo.

IV.- Que cabe también tener presente que del registro de inscripción de la URCDP surge que AA, luego de ser notificada ha reiniciado el trámite de inscripción de una de sus bases de datos denominada “Clientes de Sistema de Facturación Básico”, tal como lo exige la Ley.

V.- Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista a la empresa denunciada, así como también efectuó el traslado de sus descargos al denunciante.

CONSIDERANDO:

I- Que se trata de una situación alcanzada por la Ley N° 18.331, de 11 de agosto de 2008 y su Decreto reglamentario N° 414/009, de 31 de agosto de 2009.

II- Que el correo electrónico es considerado un dato personal de acuerdo a lo previsto en el artículo 4° literal d) de la Ley Nº 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data, que define al dato personal como “información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables”.

III. Que el artículo 21 de esta Ley a su vez expresa que, sólo es legítima la obtención de datos personales para fines de publicidad, venta u otras actividades análogas, cuando los mismos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.
IV. Que en definitiva, AA Sucursal Uruguay ha vulnerado los arts. 6°, 9°, 21 y 28 de la Ley N° 18.331.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas, así como a lo establecido en el artículo 35 de la LPDP en su redacción actual dada por el art. 152 de la Ley N° 18.719, de 27 de diciembre de 2010.
LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

RESUELVE:

I) Establecer que American Airlines Inc. Sucursal Uruguay ha vulnerado la Ley N° 18.331 al enviar correos electrónicos no solicitados por la denunciante, por lo cual se le observa.

II) Alertar acerca de la necesidad de ajustar el accionar de la empresa a lo previsto en el art. 21 de la Ley N° 18.331.

III) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde.
Consejo Ejecutivo
URCDP
g.r.

Resolución N° 1098 de 29 de julio de 2011.

Se resuelve encomendar a la Dirección de Derechos Ciudadanos de AGESIC la inspección, indagatoria y solicitud de información referidas a la inscripción de determinadas bases de datos personales.

RESOLUCION N°		EXPEDIENTE N°
1098	2011	884/2010

Montevideo, 29 de julio de 2011.

VISTO:

Las actuaciones cumplidas en múltiples expedientes de solicitud de inscripción de bases de datos personales, por quien se identifica como "tercero que realiza el tratamiento - nombre o razón social – AA – RUT… – Actividad Principal (CIU) estudio contable", conforme Item 3 de los respectivos formularios presentados.

RESULTANDO:

I) Que en los casos de referencia la Unidad ha solicitado aclaraciones y/o requerimientos informativos, a los que los administrados no han dado respuesta.

II) Que asimismo llama poderosamente la atención que, en varios casos, se opera una escueta comparecencia "por empresa" bajo firma manuscrita sin aclaración, informando que la empresa en cuestión está clausurada, sin acreditarlo en debida forma.

CONSIDERANDO:

I) Que la Unidad Reguladora en tanto órgano de control en la materia, posee potestades legales inspectivas tendientes a controlar la observancia del régimen normativo de su competencia, así como la de solicitar información de antecedentes, documentos, programas u otros elementos relativos al tratamiento de datos personales por parte de entidades públicas y privadas.

II) Que a tales efectos se solicitará a la Dirección de Derechos Ciudadanos de AGESIC el apoyo necesario para encomendar a personal técnico calificado la inspección, indagatoria de información y toda otra acción que permita esclarecer si en verdad existen -o no- existen las bases de datos personales presentadas a registro, y su regularidad jurídica.

ATENTO:

A lo expuesto y lo dispuesto por los arts. 34 lits. D) y E) de la Ley N° 18.331, de 11 de Agosto de 2008; 23 lits. C), G) y 31 A) del Decreto Nº 414/009, de 31 de Agosto de 2009.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

Encomendar a la Dirección de Derechos Ciudadanos de AGESIC la inspección, indagatoria y solicitud de información así como cualquier otra acción que permita determinar si en verdad existen -o no- las bases de datos personales presentadas a registro, y su regularidad jurídica, en los siguientes expedientes:

2010/884 – Tributa impuesto a la pequeña emp. - B B.

2010/899 – Liq. Sueldos – C C.

2010/901 – Gestión Contable – D D.

2010/905 – Liq. Sueldos – E E.

2010/907 – Gestión Contable – F F.

2010/927 – Gestión de Sueldos – G G.

2010/935 – Gestión de Sueldos – H H.

2010/936 – Recursos Humanos Sueldos – I I.

2010/3010 – Liq. De Sueldos y Contabilidad – J J.

Fdo. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

Resolución N° 1320 de 9 de setiembre de 2011.

Se resuelve postular a Uruguay como sede para la 34° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.

RESOLUCION N°		ACTA
1320	2011	29/2011

Montevideo, 9 de setiembre de 2011.

VISTO:

La institucionalidad e importancia adquiridas por las Conferencias Internacionales de Autoridades de Protección de Datos y Privacidad, como el mayor Foro dedicado a la privacidad a nivel mundial, que reúne anualmente a las máximas autoridades e instituciones garantes de la protección de datos y la privacidad, y a expertos en la materia de todos los continentes.

CONSIDERANDO:

I) Que en las ediciones Nos. 31 y 32 de esta Conferencia Internacional, celebradas en Madrid, España, y en Jerusalén, Israel, durante los años 2009 y 2010 respectivamente, Uruguay estuvo presente a través de sus autoridades en la materia.

II) Que existe consenso en destacar la importancia de este tipo de comparecencias de la Unidad, que le permite a ésta relacionarse y asumir protagonismos crecientes en las máximas instancias internacionales del sector, por todo lo que ello significa y contribuye para el mejor desarrollo y afianzamiento de un derecho, como es el derecho fundamental de la protección de datos personales y la privacidad, de naturaleza internacional y compartida con otras tantas naciones del planeta.

III) Que en tal sentido, la experiencia recogida en ediciones anteriores ha sido muy proficua y permite proyectar un paso más avanzado como es el de presentar oficialmente la candidatura de Uruguay para la edición de la Conferencia correspondiente al año 2012.

IV) Que la oportunidad para presentar esta postulación es la próxima 33ava. Conferencia Internacional, a tener lugar a fines del presente año en México.

ATENTO:

Al alto interés que reviste el evento,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

I) Postular al país como Sede de la 34ava Conferencia Internacional de Protección de Datos a celebrarse en el año 2012, teniendo presente que se deberá presentar la candidatura correspondiente en oportunidad

de la 33ava Conferencia, a fines del presente año 2011 en México.
II) Comuníquese, etc.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

Resolución N° 1321 de 15 de setiembre de 2011.

Se resuelve no hacer lugar a la denuncia contra una empresa que recopila y trata datos personales de clientes.

RESOLUCION N°		EXPEDIENTE N°
1321	2011	73/2011

Montevideo, 15 de setiembre de 2011.

VISTO:

Las actuaciones cumplidas en relación a la presente denuncia presentada originariamente ante la Comisión de Promoción y Defensa de la Competencia del Ministerio de Economía y Finanzas

RESULTANDO:

I) Que se trata de una denuncia entre empresas competidoras que prestan servicios de acompañantes a personas enfermas, para lo cual recopilan y tratan datos personales de sus clientes.

II) Que el hecho central denunciado gira alrededor de una supuesta apropiación ilegítima de clientela perteneciente a la denunciante, por parte de la denunciada.

III) Que en el decurso de las actuaciones quedó en evidencia que la denunciante integra una sociedad de hecho junto a otra socia.

CONSIDERANDO:

I) Que la Unidad Reguladora en tanto órgano de control en determinada materia, debe atenerse al principio de especialidad que fija los márgenes de su actuación, por lo que solamente le competerá pronunciarse acerca de aquellos aspectos de la denuncia y descargos, que se vinculan con el régimen jurídico de protección de datos personales (conforme Risso Ferrand, Derecho Constitucional, t.III, pág. 70 y ss. ed. Ingranusi, 1998).

II) Que en su mérito cabe centrar el asunto en las “solicitudes de afiliación” verificadas por la denunciada, las que fueron hechas con consentimiento de los titulares de datos, luciendo sus firmas respectivas y no impugnadas, lo que prueba que se cumplió con el “principio de consentimiento” en la materia, quitando todo sustento a la denuncia presentada en punto a la competencia de esta Unidad.

III) Que sin perjuicio de lo expresado, ha quedado evidenciado que tanto denunciada como denunciante han incumplido el “principio de legalidad” previsto en la Ley Nº 18.331, al realizar tratamientos de datos personales sin inscribir sus respectivas bases de datos personales, por lo que corresponde sancionarlas.

IV) Que el art. 39 inc. 1º del Código de Comercio hace responsable al socio de una sociedad de hecho, por los actos realizados por otros socios.

ATENTO:

A lo expuesto y lo dispuesto por los arts. 6°, 9°, 28, 29 y 35 de la Ley N° 18.331, de 11 de Agosto de 2008; y en el art. 39 inc. 1º del Código de Comercio,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1.- No hacer lugar a la denuncia presentada por Sedahs Ltda. en lo que atañe a la normativa de protección de datos personales.

2.- Intimar a Sedahs Ltda., María Soledad Carlos Perazza y Stefani Rosario Callero Rondan, que inscriban sus bases de datos personales en la Unidad, en el plazo de 30 días contados a partir de la notificación.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

Resolución N° 1322 de 15 de setiembre de 2011.

Se resuelve no hacer lugar a la denuncia por la cual se pone a disposición de terceros información personal en una página web del Estado.

RESOLUCION N°		EXPEDIENTE N°
1322	2011	96/2011

Montevideo, 15 de setiembre de 2011.

VISTO:

La denuncia presentada contra la Administración Nacional de Usinas y Transmisiones Eléctricas (UTE) por permitir la obtención de información de carácter confidencial entre empresa y cliente a partir de la página web del Ente mediante un dato personal no restringido, como es el número de cédula de identidad.

RESULTANDO:

I) Que conferida la vista de precepto a la denunciada, ésta se allanó deshabilitando la posibilidad expresada, quedando la información disponible solamente por medio del número de referencia de cobro.

II) Que de lo expresado por la denunciada se dio conocimiento al denunciante, quien no volvió a comparecer.

CONSIDERANDO:

I) Que la Unidad tiene potestades para expedirse en el caso, con arreglo a sus cometidos atribuidos por el art. 34 de la Ley Nº 18.331, de Protección de Datos Personales y Acción de Hábeas Data, de 11 de agosto de 2008.

II) Que el procedimiento de consulta de información a través de un sitio web, cuando involucra el suministro de datos personales, implica una actividad de tratamiento de los mismos, definida y regulada por la Ley Nº 18.331.

III) Que si bien cabe considerar el número de cédula de identidad como una especie de dato personal cuyo tratamiento no requiere consentimiento del titular conforme el art. 9º lit. C) de la Ley, de todos modos su utilización en bases de datos personales debe cumplir con los restantes postulados legales proteccionistas.

IV) Que la facilidad con que cualquier persona puede conocer el número de cédula de identidad de otra persona, hace que su utilización como medio de acceso al sistema de gestión y consulta motivo de denuncia, resulte excesiva para atender la finalidad buscada, que no es más que conocer distintos datos del servicio contratado por parte del usuario-cliente, y no por cualquier otro sujeto.

V) Que resulta pertinente y no excesiva, por el contrario, la utilización del número de referencia de cobro, en tanto se trata de un dato que permanece en la órbita de control exclusivo del usuario-cliente, adecuándose

de tal suerte a la finalidad perseguida.

VI) Que el Ente aceptó el hecho y adoptó la medida correctiva pertinente, por lo que corresponderá dar por finalizadas las presentes actuaciones, archivándolas.

ATENTO:

A lo expuesto, al Informe Letrado, y a lo dispuesto por los arts. 4º D) y M), 7º, 8º, 9º C y 34 D de la Ley N° 18.331, de 11 de Agosto de 2008.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

Tener presente el allanamiento de la denunciada, archivando las presentes actuaciones.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

Resolución N° 1338 de 7 de octubre de 2011.

Se resuelve denuncia vinculada con la existencia de cámaras de videovigilancia en ómnibus de transporte de pasajeros sin el correspondiente logo.

RESOLUCION N°		EXPEDIENTE N°
1338	2011	2011-2-10-0000140

Montevideo, 7 de octubre de 2011.

VISTO:

La denuncia realizada ante la U.R.C.D.P., con vinculación a la existencia de cámaras de videovigilancia en un ómnibus de transporte de pasajeros, sin el correspondiente logo.

RESULTANDO:

I) Que con fecha 8 de junio del corriente, presenta descargos el denunciado, indicando que las unidades de transporte no cuentan con dispositivos que generen un respaldo fílmico.

II) Que concedido el traslado de los descargos al denunciante, el mismo no se presentó.

CONSIDERANDO:

I) Que URCDP ya se pronunció en el Dictamen N° 10, de 16 de abril de 2010: "… respecto al plazo de conservación de las imágenes incide asimismo el principio de finalidad, por el cual una vez agotada la finalidad por la que se estableció el sistema de videovigilancia, se debe proceder a la eliminación de los registros realizados."
Si no existe registro de las imágenes, no puede existir tratamiento de datos.

ATENTO:

A lo precedentemente expuesto y a lo dispuesto por la Ley N° 18.331.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales.

RESUELVE:

I. ESTABLECER QUE NO EXISTIÓ CONTRAVENCIÓN DE LA LEY N°18.331 POR PARTE DE LA DENUNCIADA.
II. EXHORTAR A LA DENUNCIADA A QUE EXHIBA EN FORMA VISIBLE LOS LOGOS DISEÑADOS POR LA UNIDAD, INDICANDO LA EXISTENCIA DE LAS CÁMARAS.
III. NOTIFÍQUESE Y ARCHÍVESE.
Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
r.i.

Resolución N° 1365 de 22 de setiembre de 2011.

Se resuelve sobre la pertinencia de entregar datos a la Dirección General Impositiva.

RESOLUCION N°		EXPEDIENTE N°
1365	2011	2011-2-10-0000606

Montevideo, 22 de setiembre de 2011.

VISTO:

Estos obrados en los que se formula consulta con relación a la comunicación de datos requerida por parte de la Dirección General Impositiva al amparo de lo establecido por el Código Tributario, en especial su art. 68 ap. "E".

RESULTANDO:

Que al consultante se le ha remitido una planilla a fin de requerirle la siguiente información: "colegio, dirección, grupo familiar, número de hijos en el colegio, importe pagado por el grupo familiar en abril de 2011, nombre madre, tipo y número de documento, dirección, departamento, nombre padre, tipo y número de documento, dirección, departamento, responsable del pago, cédula de identidad u otros, dirección y observaciones".

CONSIDERANDO:

I) Que el art. 17 de la ley Nº 18.331 de 11-VIII-2008 establece que "los datos personales objeto de tratamiento 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 (…)".

II) Que resulta evidente el interés legítimo de la antes citada Administración Tributaria para el cumplimiento de los cometidos que la normativa le impone. Por su parte, el previo consentimiento del titular no es preciso cuando los datos se recaban "para el ejercicio de funciones propias de los poderes del Estado" (art. 9 "B" de la ley citada), en la especie una dependencia desconcentrada del Poder Ejecutivo-Ministerio de Economía y Finanzas, en el desarrollo de las actividades que le son inherentes.

III) Que en cuanto al requisito relativo al emisor, refiere a "fines" concernientes a circunstancias definidas de manera tal que se configura a su respecto una posición jurídica cuya legitimidad proviene de su ajuste a las reglas de derecho aplicables. En el caso de la institución consultante, es de su legítimo interés proporcionar información, aportar datos, exhibir documentación u otras formas que correspondan para acreditar el debido cumplimiento de esas reglas.

IV) Que en cuanto al mentado requisito no puede dejarse de atender la especial situación de las instituciones de enseñanza privada, que ha dado lugar a una regulación específica al mayor rango normativo, Constitución

de la República, art. 69. Ello es así, por ejemplo, en cuanto a las exigencias previstas por el art. 448 de la Ley Nº 16.226, de 29-X-1991 y a nivel administrativo por las Resoluciones de la D.G.I. Nos. 688/992, de 16-XII-1992 y 263/993, de 11-III-1993 sobre documentación correspondiente a aquellas instituciones, disposiciones que regulan la relación con la respectiva Administración.

V) Que con fecha 16 de setiembre de 2011 la D.G.I. dictó la Resolución Nº 1486/2011, en cuya parte expositiva se alude al régimen a través del cual las instituciones de enseñanza privada deben suministrar información relativa a los importes documentados vinculados a su actividad y a la conveniencia de "precisar las formalidades que deberá cumplir la documentación" de dichas instituciones.

ATENTO:

A lo expuesto, a lo establecido por la Ley de Protección de Datos y Acción de Habeas Data Nº 18.331 cuyo artículo 34 "A" prevé la competencia de esta Unidad de asesorar en esa materia.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1 - Expedirse sobre la consulta mencionada en la parte expositiva de este dictamen, en el sentido de que:
a) En el caso se configura una comunicación de datos en los términos definidos por la Ley Nº 18.331, de 11-VIII-2008.
b) La cesión de datos –desde la situación del emisor – resulta pertinente en cuanto implique cumplir con disposiciones vigentes y a los efectos indicados en el Considerando III) del presente dictamen.
c) De acuerdo con esos preceptos no fue ni es procedente la cesión de los datos específicos requeridos por la Administración Tributaria, que diera lugar a la consulta de obrados, en virtud de las normas y principios que rigen la Protección de Datos Personales.
2 - Señalar que en atención a los criterios precedentemente indicados en este dictamen, resulta procedente la cesión a que refiere la resolución mencionada en el Considerando V) respecto a los datos contenidos en la declaración jurada solicitada por la Administración Tributaria, atinentes exclusivamente al "efectivo obligado al pago".
3 - Realícense testimonios del presente dictamen a los efectos del artículo 61 del Decreto 500/991.
4 - Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

Resolución N° 1436 de 14 de octubre de 2011.

Se resuelve denuncia relativa al envío de correo electrónico no deseado.

RESOLUCION N°		EXPEDIENTE N°
1436	2011	184/2011

Montevideo, 14 de octubre de 2011.

VISTO:

La denuncia presentada por AA contra BB por envío de SPAM a la dirección de correo electrónico cc@dd.gub.uy.

RESULTANDO:

I- Que de acuerdo a la denuncia presentada, la involucrada envió publicidad sobre venta de ropa a la dirección electrónica antes mencionada.

II- Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista a la empresa denunciada, así como también efectuó el traslado de sus descargos al denunciante, realizando posteriormente los informes jurídicos correspondientes.

CONSIDERANDO:

I- Que estamos ante una situación alcanzada por la Ley N° 18.331, de 11 de agosto de 2008 y su Decreto reglamentario N° 414/009, de 31 de agosto de 2009.

II- Que corresponde hacer saber a la interesada que no resulta adecuado su accionar desde el punto de vista de la Ley de Protección de Datos Personales, ya que la finalidad de la dirección electrónica a la que se envía el correo no deseado, no es la de recibir ofertas de ropa (art. 8 de la Ley).

III- Que corresponde además que la denunciada inscriba su base de datos, de acuerdo a lo previsto en el art. 10 de la Ley.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas,

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

RESUELVE:

I) Establecer que no resulta adecuado este accionar a la Ley de Protección de Datos Personales.

II) Intimar la inscripción de la base de datos correspondiente dentro del plazo de 30 días.

III) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

g.r.

Resolución N° 1442 de 14 de octubre de 2011.

Se resuelve denuncia sobre publicación de datos personales en el sitio web del Parlamento Nacional.

RESOLUCION N°		EXPEDIENTE N°
1442	2011	334/2011

Montevideo, 14 de octubre de 2011.

VISTO:

Las actuaciones cumplidas en relación a la denuncia relativa a publicación de datos personales en el sitio web del Parlamento Nacional.

RESULTANDO:

I) Que el hecho central denunciado gira alrededor de la publicación en el expresado sitio web, de una versión taquigráfica de actuaciones realizadas en la Comisión de Hacienda de la Cámara de Senadores, donde se recogieran denuncias practicadas por un particular, denostativa de un órgano estatal y de algunos funcionarios del mismo.

II) Que la investigación administrativa instruida por el órgano afectado determinó que tales denuncias no tenían mérito.

III) Que los afectados por la información entienden que se debe eliminar la misma por ser, a su juicio, difamatoria, mientras que el órgano parlamentario involucrado alega que estará a lo que la Unidad competente en la materia resuelva (fs. 193 del expediente).

IV) Que del punto de vista técnico, las únicas formas de impedir que una información resulte indexada por los motores de búsqueda de Internet, y con ello quede accesible urbi et orbi, es su eliminación total o parcial.

CONSIDERANDO:

I) Que es del caso apreciar que ambas partes involucradas -denunciante y denunciada- muestran interés por solucionar el problema planteado.

II) Que en consonancia a dicho interés se harán valer las facultades de la Unidad para "asistir y asesorar a las personas que lo requieran" y "emitir opinión toda vez que le sea requerida a las autoridades competentes" (art. 34 lits. A) y F) de la Ley Nº 18.331).

III) Que en materia de acceso a la información pública, la doctrina especializada ha acuñado la categoría de "versión pública", operativa en los siguientes términos: "En muchos de los casos un documento o un expediente de un asunto (es decir, un conjunto de documentos agrupados) pueden contener tanto información pública como reservada o confidencial. En esta ocasión, y para dar vigencia al principio de máxima publicidad, se puede elaborar lo que se conoce como `versiones públicas´. Esto significa

simplemente que las partes reservadas o confidenciales del documento o del expediente se testan (tachan) o se eliminan. Esto permite dar acceso a la información al tiempo que se mantiene en reserva respecto de las cuestiones que tiene este carácter" (Sergio LÓPEZ AYLLON - "El acceso a la información como un derecho fundamental: la reforma al artículo 6º de la Constitución mexicana", Cuaderno de Transparencia Nº 17 del IFAI - http://www.ifai.org.mx/Publicaciones/publicaciones)

ATENTO:

A lo expuesto y lo dispuesto por los arts. 1º, 2º, 7º, 15, 16, 31 y 34 lits. A) y F) de la Ley N° 18.331, de 11 de Agosto de 2008.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1.- Sugerir a la autoridad respectiva que disponga la baja de su sitio web de los documentos motivantes de la denuncia, sustituyéndolos por otros de igual tenor donde figuren tachados o eliminados los nombres del órgano y funcionarios afectados (versión pública).

2.- Hacer saber que la armonización del principio de máxima publicidad de la información pública con la co-existencia de datos confidenciales o reservados (entre otros "datos personales") es resorte y cometido de los jerarcas de los órganos que ordenan aquella publicidad, a resolver y poner en práctica conforme intereses y deberes propios de su competencia, no constituyendo la presente resolución más que una guía u orientación facilitadora al efecto.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

Resolución N° 1443 de 21 de octubre de 2011.

Se resuelve denuncia presentada por correo electrónico no deseado.

RESOLUCION N°		EXPEDIENTE N°
1443	2011	2011-2-10-0000095

.

Montevideo, 21 de octubre de 2011.

VISTO:

La denuncia presentada por envío de correo no solicitado.

RESULTANDO:

I.- Que se dio trámite a la misma, dando oportunidad a la denunciada para que formulara sus descargos.

II.- Que en su comparecencia la denunciada sostiene que puede haberse tratado de un reenvío de su correo publicitario al denunciante, por parte de alguien que lo recibió directamente y pensó que podría interesarle al denunciante; y en cuanto a la repetición de tales envíos, no obstante el pedido de exclusión del denunciante, que pudo obedecer a “error informático”.

CONSIDERANDO:

I.- Que las explicaciones ofrecidas no satisfacen ni alcanzan para desmentir la infracción cometida, encontrándonos ante un caso de lo que en doctrina se denomina “spam”, vale decir comunicación no solicitada realizada por vía electrónica.

II.- Que la hipótesis así encuadrada configura un incumplimiento del art. 21 de la Ley Nº 18.331 en su actual redacción dada por el art. 152 de la Ley Nº 18.719, ya que el correo del denunciante es un dato personal, y el mismo no fue tomado de un documento accesible al público, ni facilitado por su titular, ni obtenido con su consentimiento.

III.- Que consta, asimismo, que la denunciada no ha inscripto su/s base/s de datos/s personales ante esta Unidad, conforme ordenan los arts. 28 y 29 de la Ley Nº 18.331 en sus respectivas redacciones actuales dadas respectivamente por los arts. 152 y 154 de la Ley Nº 18.719.

IV.- Que atendiendo la primariedad de los ilícitos cometidos, corresponde aplicar la sanción mínima dentro de la escala legalmente vigente, e intimar la inscripción antes mencionada.

ATENTO:

A lo expuesto, al Informe Letrado agregado, y a lo dispuesto por los artículos 1°, 4° D), 21, 28, 29 y 35 1) de la Ley N° 18.331 y su modificativa Ley Nº 18.719.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

I) SANCIONAR CON "OBSERVACIÓN" A LA EMPRESA LOGTRA LTDA. POR INFRACCIÓN A LA LEY Nº 18.331 (ENVÍO DE CORREOS NO SOLICITADOS).
INTIMAR A LA MISMA EMPRESA EL REGISTRO DE LA/S BASE/S DE DATO/S PERSONALES QUE DISPONGA, EN EL PLAZO DE TREINTA DÍAS CORRIDOS BAJO APERCIBIMIENTO DE MAYORES SANCIONES SI NO LO HICIERE.
NOTIFÍQUESE Y PUBLÍQUESE.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

Resolución N° 1473 de 28 de octubre de 2011.

Se resuelve denuncia presentada por correo electrónico no deseado.

RESOLUCION N°		EXPEDIENTE N°
1473	2011	522/2011

Montevideo, 28 de octubre de 2011.

VISTO:

La denuncia presentada por envío de correos no solicitados.

RESULTANDO:

I.- Que se dio trámite a la misma, dando oportunidad a la denunciada para que formulara sus descargos.

II.- Que la denunciada tomó la vista correspondiente pero no presentó escrito de descargos.

CONSIDERANDO:

I.- Que la hipótesis encuadra como "spam", vale decir comunicación no solicitada realizada por vía electrónica, habiendo el denunciante solicitado que se borre su dirección de correos de la lista respectiva, sin éxito.

II.- Que la situación que padece el denunciante así encuadrada, configura un incumplimiento del art. 21 de la Ley Nº 18.331 en su actual redacción dada por el art. 152 de la Ley Nº 18.719, ya que su correo electrónico es un dato personal, y el mismo no fue tomado de un documento accesible al público, ni facilitado por su titular, ni obtenido con su consentimiento.

III.- Que consta, asimismo, que la denunciada no ha inscripto su/s base/s de datos/s personales ante esta Unidad, conforme ordenan los arts. 28 y 29 de la Ley Nº 18.331 en sus respectivas redacciones actuales dadas respectivamente por los arts. 152 y 154 de la Ley Nº 18.719.

IV.- Que atendiendo la primariedad de los ilícitos cometidos, corresponde aplicar la sanción mínima dentro de la escala legalmente vigente, e intimar la inscripción antes mencionada.

ATENTO:

A lo expuesto, al Informe Letrado agregado, y a lo dispuesto por los artículos 1°, 4° D), 21, 28, 29 y 35 1) de la Ley N° 18.331 y su modificativa Ley Nº 18.719.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

I) SANCIONAR CON "OBSERVACIÓN" A LA ASOCIACIÓN URUGUAYA DE FÚTBOL POR INFRACCIÓN A LA LEY Nº 18.331 (ENVÍO DE CORREOS NO SOLICITADOS).

II) INTIMAR A LA MISMA INSTITUCIÓN EL REGISTRO DE LA/S BASE/S DE DATO/S PERSONALES QUE DISPONGA, EN EL PLAZO DE TREINTA DÍAS CORRIDOS BAJO APERCIBIMIENTO DE MAYORES SANCIONES SI NO LO HICIERE.

III) NOTIFÍQUESE Y PUBLÍQUESE.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

Resolución N° 1492 de 4 de noviembre de 2011.

Se resuelve denuncia sobre envío de correo electrónico no deseado.

RESOLUCION N°		EXPEDIENTE N°
1492	2011	182/2011

Montevideo, 4 de noviembre de 2011.

VISTO:

La denuncia presentada ante esta unidad contra AA por el envío de correos electrónicos promocionales no deseados.

RESULTANDO:

I) Que con fecha 18 de agosto del corriente se presenta la denunciada a manifestar que por un error (a la fecha solucionado), no se encontraba el "checkbox" en la página mencionada.

II) Que dado traslado de los descargos al denunciante, el mismo no se presentó.

CONSIDERANDO:

I) Que para que los datos puedan ser tratados, se requiere el consentimiento previo del titular, en los términos del artículo 9° de la Ley N° 18.331.

II) Que existe por parte de las empresas la obligación de informar sobre sus derechos a las personas incluidas en la base de datos, atento a lo establecido en el artículo N° 14 de la citada Ley.

ATENTO:

A lo precedentemente expuesto y a lo dispuesto por le Ley N° 18.331.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales.

RESUELVE:

I. SE SUGIERE RECOMENDAR AL DENUNCIANTE EL QUE EJERZA SU DERECHO DE ACCESO EN LOS TÉRMINOS DEL ARTÍCULO 14 DE LA LEY N° 18.331, A FIN DE CONSTATAR SI SUS DATOS FUERON ELIMINADOS.

II. SE SUGIERE RECOMENDAR A GANISOL S.A. EL RECABAR EL CONSENTIMIENTO DE SUS USUARIOS, EN LOS TÉRMINOS DEL ARTÍCULO 9° DE LA LEY N° 18.331.
III. NOTIFÍQUESE Y PUBLÍQUISE.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
r.i.

Resolución N° 1538 de 11 de noviembre de 2011.

Se resuelve aprobar el anteproyecto normativo para la protección de datos personales en el ámbito del MERCOSUR.

RESOLUCION N°		EXPEDIENTE N°
1538	2011	2947/2010

Montevideo, 11 de noviembre de 2011.

VISTO:

El Anteproyecto normativo para la protección de datos personales en el ámbito del MERCOSUR, sometido a examen de la Unidad a partir de la iniciativa proveniente del SGT Nº 13.

CONSIDERANDO:

I.- Que se considera relevante la regulación de la temática abordada, como parte del proceso de integración regional.

II.- Que en tal sentido, y luego del examen técnico correspondiente, se entiende oportuno y meritorio aprobar el texto sometido a examen, con algunas modificaciones respecto de su versión original.

ATENTO:

A lo precedentemente expuesto, a lo informado por los Asesores Letrados y a lo dispuesto por los arts. 31 y 34 B) de la Ley Nº 18.331, de 11 de Agosto de 2008.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1.- Aprobar el Anteproyecto normativo para la protección de datos personales en el ámbito del Mercosur, de acuerdo al texto del mismo que figura en Anexo a la presente Resolución y se considera parte de la misma..

2.- Cúrsense las comunicaciones y publicaciones del caso.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

Anexo Res. Nº 1538 de 11-11-2011 URCDP

ANTEPROYECTO DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO DEL MERCOSUR

Capítulo I – Disposiciones Generales

Artículo 1. Objeto

Los Estados Partes garantizarán, con arreglo a las disposiciones de la presente ..., la protección integral de los datos de las personas físicas asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre. Los Estados Partes podrán extender estas garantías a las personas jurídicas en lo que consideren pertinente.

Artículo 2. Definiciones

A efectos del presente Acuerdo, se entenderá por:

Datos personales: Información de cualquier tipo referida a personas físicas determinadas o determinables.

Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Archivo, registro, base o banco de datos: 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.

Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general el procesamiento de datos personales, así como también su cesión a terceros a través de transferencias, comunicaciones, consultas o interconexiones.

Responsable del archivo, registro, base o banco de datos: Persona física o jurídica, pública o privada, que es titular de un archivo, registro, base o banco de datos.

Titular de los datos: Toda persona física cuyos datos sean objeto del tratamiento al que se refiere el presente Acuerdo.

Usuario de datos: toda persona pública o privada, que realice a su arbitrio el tratamiento de datos ya sea en una base de datos propia o a través de conexión con los mismos.

Encargado de tratamiento: 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.

Consentimiento del titular: toda manifestación de voluntad, libre, específica e informada, mediante la que el titular consienta el tratamiento de datos personales que le conciernan.

Artículo 3. Ámbito de aplicación

Las disposiciones de la presente ... no se aplicarán al tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Los Estados Partes

podrán exceptuar la aplicación de la presente ... al tratamiento de datos que tenga por objeto la seguridad pública, la defensa nacional, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito, así como las bases de datos creadas y reguladas por leyes especiales.

Artículo 4. Ámbito territorial

Los Estados Partes aplicarán las disposiciones nacionales que hayan aprobado para poner en práctica la presente ..., cuando:

a) el tratamiento de los datos sea efectuado en el marco de las actividades de un responsable de archivo, registro, base o banco de datos que actúa en el territorio del respectivo Estado Parte, aún cuando el banco de datos éste radicado físicamente fuera de dicho territorio. Cuando el mismo responsable éste establecido en el territorio de varios Estados Partes deberá adoptar las medidas necesarias para garantizar que cada uno de los archivos, registros, bases o bancos de datos cumpla las obligaciones previstas por el derecho nacional aplicable;

b) el responsable del archivo, registro, base o banco de datos no esté establecido en el territorio del Estado Parte, sino en un lugar en que se aplica su legislación nacional en virtud del derecho internacional;

c) el responsable del archivo, registro, banco o base de datos no esté establecido en el territorio de alguno de los Estados Partes y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dichos Estados.

Exceptúanse de la regla precedente, los casos en que los citados medios se utilicen exclusivamente con fines de tránsito, siempre que el responsable de la base de datos o tratamiento designe un representante con domicilio y residencia permanente en el territorio del Estado parte, ante su órgano de control, a los efectos de cumplir con las obligaciones previstas por la presente .... Tal designación no impedirá las acciones legales que puedan ser promovidas contra el responsable de la base de datos o tratamiento ni disminuirá su responsabilidad en cuanto al cumplimiento de las obligaciones impuestas legal o reglamentariamente.

Capítulo II Disposiciones generales para la licitud del tratamiento de datos personales

Artículo 5. Licitud del tratamiento

Los Estados Partes establecerán las condiciones para que el tratamiento de datos personales se considere lícito.

Las condiciones de licitud deberán respetar los principios establecidos por el presente Acuerdo.

Artículo 6. Calidad de los datos

Los Estados Partes dispondrán que:

Los datos personales que se recojan a los efectos de su tratamiento sean ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

La recolección de datos no se efectúe por medios desleales, fraudulentos o en forma contraria a las disposiciones internas que se dicten en virtud del presente Acuerdo.

Los datos objeto de tratamiento no sean utilizados para finalidades distintas o incompatibles con áquellas que motivaron su obtención.

Los datos sean exactos y se actualicen en el caso de que ello fuere necesario.
Los datos sean almacenados de modo que permitan al titular el ejercicio de los derechos de acceso, rectificación, actualización, supresión y confidencialidad.
Los datos sean destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Artículo 7. Consentimiento

1. Los Estados Partes establecerán que el tratamiento de datos personales será lícito cuando el titular hubiere prestado su consentimiento previo, libre, expreso e informado, en las condiciones que las legislaciones nacionales dispongan.
2. Los Estados Partes podrán exceptuar el consentimiento cuando lo consideren necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el sujeto o sujetos a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del titular del dato.

Artículo 8. Tratamiento de datos sensibles

Los Estados Partes prohibirán el tratamiento de datos sensibles y establecerán las excepciones y condiciones para su tratamiento, asegurándoles una especial protección.

Artículo 9. Tratamiento de datos personales y libertad de expresión

Los Estados Partes garantizarán la no afectación de las fuentes periodísticas.

Artículo 10. Derecho de acceso

Los Estados Partes garantizaran que el titular de los datos tenga derecho a solicitar y obtener información de sus datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados. El derecho a que se refiere este artículo deberá poder ser ejercido libremente, sin restricciones y con una periodicidad razonable. La información suministrada al titular en ejercicio de este derecho, deberá ser clara e inteligible, amplia y referida a la totalidad del registro perteneciente al titular.

Artículo 11. Derecho de rectificación, actualización, supresión y confidencialidad.

Los Estados Partes deben garantizar que toda persona tenga derecho a que sus datos personales incluidos en archivos, registros, bancos o bases de datos puedan ser rectificados, actualizados y cuando corresponda, suprimidos o sometidos a confidencialidad, cuando el tratamiento de datos personales no se ajuste a los principios establecidos por el presente Acuerdo.
En el supuesto de cesión o transferencia de datos, el responsable o usuario del banco de datos estará obligado a notificar la rectificación o supresión al cesionario.

Artículo 12. Excepciones oponibles al titular del dato

Los Estados Partes podrán adoptar medidas legales para limitar los derechos previstos en los artículos 10 y 11, cuando tal limitación constituya una medida necesaria para la salvaguarda de:

a) seguridad del Estado, defensa y seguridad pública;

b) protección de derechos y libertades de otras personas;

c) actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre cumplimiento de obligaciones tributarias o previsionales, delitos penales, infracciones administrativas, funciones de control de la salud o del medio ambiente.

Artículo 13. Gratuidad.

Los derechos de acceso, rectificación, actualización o supresión de datos personales inexactos, incompletos, excesivos o no pertinentes que obren en archivos, registros, bases o bancos de datos públicos o privados se ejercerán sin cargo alguno para el interesado.

Artículo 14. Derecho de oposición del titular del dato

Los Estados Partes reconocerán al titular del dato el derecho a oponerse, en cualquier momento y por razones fundadas propias de su situación particular, a que sus datos sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso que la oposición sea pertinente, el tratamiento que efectúe el responsable no podrá volver a referirse a esos datos.

Artículo 15. Decisiones individuales automatizadas

Los Estados Partes garantizarán que las personas no quedarán sujetas a decisión alguna que tenga efectos jurídicos sobre ellas, o que les afectare de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluarlas. Solamente se aceptará dicho tratamiento cuando por contrato o ley se garantice la efectiva protección de los derechos e interés legítimo del titular.

Artículo 16. Confidencialidad del tratamiento

Los Estados Partes deberán garantizar que el responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales estén obligados a guardar secreto de los mismos, obligación que subsistirá aún después de finalizada su relación con el responsable del archivo, registro, base o banco de datos. La obligación de guardar secreto podrá ser relevada por resolución judicial o cuando medien razones de seguridad pública, defensa nacional o salud pública.

Artículo 17. Seguridad del tratamiento

Los Estados Partes establecerán que el responsable o usuario de archivos, registros, bases o bancos de datos adopte las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, acceso, consulta o tratamiento no autorizado y que permitan detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado, quedando prohibido registrar datos personales en archivos, registros, bases o bancos de datos que no reúnan condiciones técnicas de integridad y seguridad.

Artículo 18. Transferencia internacional

1. Los Estados Partes se comprometen a prohibir la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales que no proporcionen niveles adecuados de protección conforme a lo establecido en la presente.

2. El carácter de adecuado del nivel de protección que ofrece un país tercero, se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencia de datos; en particular, se tomarán en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

3. Sin perjuicio de lo dispuesto en el numeral 1 del presente artículo, los Estados Partes podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección adecuado con arreglo a los numerales 2 y 3 del artículo 17, cuando el responsable del archivo, registro, banco o base de datos ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos, dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas

6. Los Estados Partes podrán disponer las excepciones a la prohibición establecida en el punto 1 del presente artículo, siempre que se otorguen garantías adecuadas de protección de los datos personales.
Los Estados Partes determinarán los requisitos del procedimiento de autorización señalado.

Artículo 19. Deber de registro

Los Estados Partes dispondrán que todo archivo, registro, base o banco de datos personales deberá inscribirse en los registros que al efecto habiliten los órganos de control de cada uno de ellos.

Podrán disponer la simplificación u omisión del deber de registro sólo en aquellos casos previstos en la legislación interna de cada uno de ellos, siempre y cuando no se afecten derechos y libertades de los titulares de los datos, se precisen las categorías de tratamiento a excluir y se reglamenten dichos procesos y situaciones.

Capítulo III – Recursos judiciales, responsabilidad y sanciones

Artículo 20. Recursos

Los Estados Partes establecerán que toda persona disponga de una vía administrativa ante el órgano de control local, así como también de una instancia judicial sumarísima en caso de violación de los derechos garantizados en este Acuerdo.

Artículo 21. Sanciones

Los Estados Partes adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente y determinarán, en particular, las sanciones administrativas que deben aplicarse en caso de su incumplimiento.

Capítulo IV – Códigos de Conducta

Artículo 22. Códigos de Conducta

Los Estados Partes propiciarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones del presente Acuerdo. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el órgano de control, quien podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones sobre la materia.

Capítulo V Órgano de Control

Artículo 23. Órgano de control

1.Los Estados Partes dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente .... Estas autoridades ejercerán sus funciones con plena autonomía técnica.

2. Los Estados Partes dispondrán que se consulte a los respectivos órganos de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

3. Los órganos de control poseerán las siguientes funciones y atribuciones:

a) Asesorar a quienes lo requieran acerca de sus derechos en materia de protección de datos personales.

b) Promover la difusión de información relativa al derecho a la protección de datos personales.

c) Realizar y mantener un registro permanente de los archivos, registros, bases o bancos de datos.

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros, bases o bancos de datos.

e) Ejercer poderes de investigación y solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran, y acceder a locales, equipos, o programas de tratamiento de datos conforme requisitos y garantías contenidos en la ley nacional respectiva, a fin de verificar infracciones al cumplimiento de la normativa aplicable en la materia.

f) Imponer las sanciones administrativas que en su caso correspondan por violación a la normativa aplicable en la materia.

Capítulo VI – Disposiciones Finales

Artículo 24. Vigencia

El presente Acuerdo entrará en vigor treinta (30) días después de la fecha de depósito del tercer instrumento de ratificación.

Artículo 25. Depositario

El Gobierno de la República del Paraguay será depositario del presente Acuerdo y enviará copias debidamente autenticadas a los gobiernos de los demás Estados signatarios.

Resolución N° 1658 de 7 de diciembre de 2011.

Se resuelve denuncia sobre publicación en Internet de una sanción impuesta al denunciante por quien ejerce la superintendencia de su profesión, y la falta de baja o eliminación una vez cumplida.

RESOLUCION N°		EXPEDIENTE N°
1658	2011	2011-2-10-0000079

Montevideo, 7 de diciembre de 2011.

VISTO:

La denuncia presentada en relación a la publicación en Internet de una sanción aflictiva del denunciante, y su falta de baja o eliminación una vez cumplida la misma.

RESULTANDO:

I) Que la denuncia en cuestión hace referencia a la suspensión del afectado en el ejercicio de las profesiones de Abogado y Procurador, dispuesta por la Suprema Corte de Justicia en los términos establecidos por el artículo 140 de la Ley Nº 15.750.

II) Que las resoluciones respectivas, tanto la que contiene la sanción aplicada como aquélla que dispuso la rehabilitación del sancionado, son recuperables a través de los motores de búsqueda disponibles en Internet, como Google.

III) Que estos motores de búsqueda indexan aquellos archivos que se suben a la Red por parte de quienes los generan o reproducen, y consecuentemente dejan de hacerlo cuando el archivo es eliminado o bajado de la misma.

IV) Que en el ocurrente, si bien se eliminó el nombre del denunciante del registro de profesionales suspendidos presente en la Red, de todos modos la publicidad tangencial de los mismos hechos (suspensión y rehabilitación) continuó vigente, a través de la publicación de las Circulares que dan cuenta de los mismos hechos, desvirtuándose de este modo la supuesta eliminación del registro de sancionados.

V) Que los hechos así ocurridos afectan al denunciante en el ejercicio de su profesión, tratándose -por lo demás- de una sanción conexa a un delito de lesiones personales declarado extinguido al cabo de la instrucción respectiva, lo que amplifica el agravio.

CONSIDERANDO:

I) Que la publicidad o difusión de datos personales a través de Internet, configura una especie de tratamiento de datos que, como tal, debe cumplir con los postulados del régimen objeto de tutela, en particular que "los datos personales que se recogieren... deberán ser... no excesivos en relación con la finalidad para la cual se hubieren obtenido" (arts. 4º lit. M), 7º y 8º de la Ley Nº 18.331, de 11 de agosto de 2008).

II) Que la permanencia sine die de este tipo de información en Internet, ya sea en forma de registros específicos (por vía de la planilla de profesionales suspendidos y rehabilitados) como en forma oblicua o tangencial (por vía de la base de datos de "Circulares del Poder Judicial"), no se compadece con la regulación legal anotada.

III) Que en cumplimiento del principio de responsabilidad corresponde al Poder Judicial encontrar la fórmula técnico-legal adecuada para que la publicidad o difusión de sanciones y rehabilitaciones de profesionales suspendidos en el ejercicio de su profesión, resulte compatible con el régimen jurídico de protección de los datos personales.

IV) Que procede advertir acerca de la no inscripción de las bases de datos personales que dispone la denunciada, entre ellas la alusiva a los hechos motivantes de estas actuaciones.

ATENTO:

A lo expuesto y lo dispuesto por los arts. 1º, 4º A) K) y M), 8º, 12 y 24 de la Ley N° 18.331, de 11 de Agosto de 2008.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1.- Declarar que asiste razón al denunciante por lo que se entiende acorde a derecho que el Poder Judicial-Suprema Corte de Justicia suprima los datos personales del mismo vinculados a decisiones de suspensión y rehabilitación en el ejercicio de las profesiones de Abogado y Procurador, en todos aquellos archivos volcados a la Red Internet cualquiera sea su forma.

2.- Sugerir la necesidad y conveniencia de ajustar para el futuro, el mecanismo de publicidad o difusión de sanciones y rehabilitaciones a profesionales suspendidos en el ejercicio de su profesión, a fin de adecuarlo al cumplimiento de las normas y principios generales vigentes en materia de protección de datos personales.

3.- Hacer saber a la Suprema Corte de Justicia – Poder Judicial lo expresado en el Considerando IV) de la presente Resolución.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

Dictamen N° 2 de 4 de febrero de 2011.

Se dictamina sobre la creación de una base de datos para contactos.

DICTAMEN N°		EXPEDIENTE N°
2	2011	01/2011

Montevideo, 4 de febrero de 2011.
Ref. Consulta sobre la creación de base de datos.

VISTO:

Estas actuaciones relativas al Sr. Hugo Álvarez en cuanto a la creación de una base de datos personales

RESULTANDO:

Que fueron remitidas por la Unidad Reguladora y de Servicios y Comunicaciones (URSEC) con fecha 3 de enero de 2011 y se realizó el informe jurídico Nº 137 con fecha 11 de enero de 2011 (fs. 26 a 28).

CONSIDERANDO:

I.- Que de la consulta planteada se desprende que, el consultante se constituiría en responsable de la base de datos, y que ésta contendría datos identificatorios correspondientes a personas físicas, dentro de los cuales se encuentran, el nombre, domicilio y teléfono celular.
Que asimismo se desprende de la información proporcionada, que las finalidades de tratamiento y comunicación versan sobre el contacto y ubicación de personas físicas.

II.- Que como responsable de la base de datos, debe cumplir con las obligaciones previstas en la Ley N° 18.331, fundamentalmente las correspondientes con el deber de inscripción de la base de datos, respeto de los principios generales en la materia, y contar con mecanismos adecuados para el ejercicio de los derechos de los titulares de los datos personales.

III.- Que el artículo 6° de la Ley N° 18.331, prevé que la formación de base de datos es lícita cuando éstas se encuentren debidamente inscriptas
Que sin perjuicio que el deber de inscripción de las bases de datos creadas con posterioridad a la aprobación del Decreto N° 414/009, de 31 de agosto de 2009, puede ser cumplido en el plazo de 90 días, se entiende que en el caso el cumplimiento de dicho deber corresponda sea efectuado a la brevedad, a los efectos de que, una vez cumplidas las etapas del procedimiento administrativo de registro de bases de datos, se resuelva de forma definitiva acerca de la adecuación de la base de datos a la normativa vigente.

IV.- Que en cuanto a la documentación presentada, corresponde tener presente que en el sitio web de la Unidad, se encuentran disponibles para su descarga, los formularios para la recolección del consentimiento informado y el ejercicio de los derechos de los titulares. Sin perjuicio de ello, los formularios confeccionados por el consultante, podrán ser presentados a efectos de su análisis en cuanto a su adecuación a los parámetros legales y reglamentarios que rigen en la materia.

ATENTO:

A lo expuesto y a lo establecido por los artículos 4° literal a) y k), 6°, 7°, 8°, 9°, 10, 11, 13, 14, 15 y 29 de la Ley N° 18.331, y los artículos 15 literal a) y 17 del Decreto N° 414/009.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

Expedirse en el sentido indicado en la parte expositiva del presente, específicamente en los Considerandos Nos. II) y III).

Notifíquese al interesado.

Publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo
URCDP
f.c.

Dictamen N° 3 de 10 de febrero de 2011.

Se dictamina sobre consulta del Comité Uruguayo de Seguridad Bancaria respecto a la posibilidad de no aplicar la Ley en los circuitos cerrados de televisión de instituciones bancarias.

DICTAMEN N°		EXPEDIENTE N°
3	2011	2010/3562

Montevideo, 10 de febrero de 2011.

VISTO:

La consulta formulada por el Comité Uruguayo de Seguridad Bancaria (CUSEBA).

RESULTANDO:

I) Que CUSEBA solicita a la Unidad Reguladora y de Control de Datos Personales, se expida acerca de si los sistemas de circuitos cerrados de televisión (CCTV) instalados en las instituciones bancarias, se encuentran amparados en la excepción prevista en el literal B) del artículo 3° de la Ley N° 18.331.

II) Que se expidió el informe jurídico N° 5200 de 29 de diciembre de 2010.

CONSIDERANDO:

I) La Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP) define base de datos como el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuera la modalidad de su formación, almacenamiento, organización o acceso. Y dato personal, como información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. (artículo 4°, literales A) y D).

II) Los sistemas de videovigilancia instalados en las entidades consultantes, en tanto permiten la grabación, captación, transmisión, conservación y/o almacenamiento de imágenes de una persona determinada o determinable, hacen aplicable la normativa proteccionista de datos personales.

III) El artículo 3° de la LPDP delimita el ámbito objetivo de la Ley, estableciendo que su régimen será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.
Añade tal disposición que no será de aplicación, entre otras, a las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito. (literal B). Esta norma es reproducida en el Decreto Reglamentario de la Ley, Nº 414/009, de 31 de agosto de 2009, artículo 2° literal B).

IV) Conforme lo prevé la Circular N° 1564/97 del Banco Central del Uruguay, que sustituye el artículo 32 de la Recopilación de Normas de Regulación y Control del Sistema Financiero, las empresas de intermediación

financiera deberán ajustarse estrictamente a lo dispuesto por el artículo 13 del Decreto N° 416/985, adoptando los requisitos de seguridad impuestos por el Ministerio del Interior.
Tales disposiciones se suman a otras normas como la Ley de prevención de lavado de activos (Ley N° 17.835 y su modificativa N° 18.494) y la Ley N° 15.322, art. 25, relativa al secreto bancario, que refuerzan la idea de que la instalación de sistemas de circuito cerrado de televisión (CCTV) o videovigilancia en las entidades financieras, responden a motivos de seguridad pública que deben observarse.
La habilitación de los locales bancarios depende de la instalación de sistemas de CCTV con grabación de video, con el cumplimiento de determinados requisitos como es el mantenimiento de dichas imágenes por un período determinado, estando a disposición de las autoridades competentes la entrega de éstas, en el caso de serle requerido.

ATENTO:

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

DICTAMINA:

1) Expedirse en el sentido que los sistemas de circuito cerrado de televisión (CCTV) o videovigilancia que se encuentren instalados en las entidades financieras públicas o privadas, por imposición de la normativa del Ministerio del Interior y del Banco Central del Uruguay, en tanto se sustentan en razones de "seguridad pública", resultan exceptuados del régimen de la LPDP, al amparo de lo previsto en su artículo 3° literal B). Por tanto, no les asiste la obligación de inscripción ante la Unidad Reguladora y de Control de Datos Personales.
No obstante, resulta aconsejable que las entidades involucradas:
a) incorporen en lugares visibles, los logos de videovigilancia aprobados por Resolución N° 989/010, de 30 de julio de 2010, a los cuales se puede acceder a través del sitio web www.datospersonales.gub.uy.
b) tengan presente los principios rectores en materia de protección de datos personales, de veracidad, finalidad, seguridad y reserva, regulados en los artículos 7°, 8°, 10 y 11 de la LPDP.
2) Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo
URCDP

m.j.r.

Dictamen N° 4 de 17 de febrero de 2011.

Se dictamina sobre consulta de Compras y Contrataciones Estatales de AGESIC en relación con la procedencia del registro de la base de datos de usuarios que utiliza el Sistema Informático de Compras Estatales (SICE).

DICTAMEN N°		EXPEDIENTE N°
4	2011	2011/19

Montevideo, 17 de febrero de 2011.

VISTO:

La consulta formulada por Compras y Contrataciones Estatales de AGESIC, acerca de si corresponde registrar la base de datos personales de usuarios (funcionarios públicos) que utilizan el SICE y la página www.comprasestatales.gub.uy

RESULTANDO:

I.- Que se trata de dependencias de la Administración Pública que deben publicar los procedimientos de compras en los referidos sistemas informáticos, registrándose a tales efectos los datos de funcionarios (nombre y apellido, teléfono de la oficina, entre otros).

II.- Que estos datos son los mínimos necesarios para ingresar al sistema informatizado, estando agrupados y registrados bajo la forma de "base de datos" con arreglo a la definición legal que proporciona el art. 4º lit. A) de la Ley Nº 18.331, según amplía y aclara la consultante en segunda comparecencia.

CONSIDERANDO:

I.- Que conforme el art. 29 de la Ley Nº 18.331 "toda base datos pública o privada debe inscribirse en el Registro que al efecto habilite el Órgano de Control, de acuerdo a los criterios reglamentarios que se establezcan".

II.- Que la base de datos objeto de consulta no entra en ninguna de las hipótesis de inaplicabilidad de la Ley contempladas en su art. 3º.

ATENTO:

A lo expuesto y a lo dispuesto por los artículos 3º, 4º A), y 29 de la Ley N° 18.331; 1º del Decreto Nº 664/008 y 15 del Decreto Nº 414/009.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

I) QUE LA BASE DE DATOS DE USUARIOS REQUERIDA Y CONFECCIONADA PARA EL INGRESO AL SICE Y A LA PÁGINA www.comprasestatales.gub.uy, DEBE INSCRIBIRSE EN EL REGISTRO DE BASES DE DATOS QUE LLEVA ESTA UNIDAD.

II) NOTIFÍQUESE Y PUBLÍQUESE.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo
URCDP

m.b.

Dictamen N° 5 de 1 de abril de 2011.

Se dictamina sobre la posibilidad de eliminar información de tipo comercial regulada por el artículo 22 de la Ley N° 18.331.

DICTAMEN N°		EXPEDIENTE N°
5	2011	47/2011

Montevideo, 1 de abril de 2011.

VISTO:

La consulta presentada por el Sr. Andrés Medeiros.

RESULTANDO:

I) Que el Sr. Medeiros solicita la intervención de la Unidad Reguladora y de Control de Datos Personales a efectos de que se le informe sobre la procedencia de la inscripción de una deuda en la base de datos de Clearing de Informes, así como de los medios legales que dispone para la defensa de sus derechos, al amparo de lo previsto por el artículo 34 lit. A) de la Ley N° 18.331.

II) Que se expidió el informe jurídico N° 4722 de 22 de marzo de 2011.

CONSIDERANDO:

I) La Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP) prevé en el artículo 22 que "Los datos personales relativos a obligaciones de carácter comercial de personas físicas solo podrán estar registrados por un plazo de cinco años contados desde su incorporación. En caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original. Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción".

II) Conforme lo manifestado por el consultante, la solicitud de registro a Clearing de Informes por parte de la empresa acreedora se hizo el 27 de diciembre de 2001 y ésta es la que debe tenerse en cuenta para comenzar a computar el plazo de conservación del registro, conforme lo dispuesto por el referido artículo 22 que alude: "...desde su incorporación". En consecuencia, la permanencia de tal asiento por el plazo de 10 años sería válida hasta el 27/12/2011.

ATENTO:

A lo expuesto y lo dispuesto por las disposiciones legales citadas,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido que de acuerdo con los elementos que obran en estas actuaciones, corresponde esperar al vencimiento del plazo de diez años previsto por el artículo 22 de la LPDP (27 de diciembre de 2011) a fin de efectuar una solicitud de acceso ante Clearing de Informes -al amparo de lo previsto por el artículo 14 de la LPDP- para constatar que se haya eliminado la información.

2) Señalar que para el ejercicio del derecho de acceso ante Clearing de Informes, se podrá utilizar el modelo diseñado por la URCDP a tales efectos, ingresando, a través de su sitio web, al siguiente link: http://www.datospersonales.gub.uy/sitio/pdf/Formulario_para_ejercer_el_derecho_de_acceso.pdf

3) Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo
URCDP

m.j.r.

Dictamen N° 6 de 26 de mayo de 2011.

Se dictamina sobre el procedimiento de inspección de las empresas amparadas por el secreto profesional.

DICTAMEN N°		EXPEDIENTE N°
6	2011	52/2011

Montevideo, 26 de mayo de 2011.
Ref. Consulta sobre cómo va a proceder la URCDP con la información de las empresas amparadas por el secreto profesional en el marco de las inspecciones que se realicen.

VISTO:

La consulta formulada a propósito de la compatibilidad entre las facultades de fiscalización e inspección de la Unidad Reguladora y de Control de Datos Personales, y el deber de confidencialidad de los Asesores de Inversión sobre los datos personales de sus clientes plasmado en el llamado “secreto profesional”.

RESULTANDO:

I- Que el art. 34 lit. D) de la Ley Nº 18.331 en su redacción actual dada por el art. 155 de la Ley Nº 18.719, prevé y regula las facultades de la Unidad en materia de fiscalización e inspección de las bases de datos personales sometidas a su control.
II- Que entre dichas facultades están las de exigir a responsables y encargados la exhibición de todo tipo de documentación, tradicional o digital, intervenir el material inspeccionado, tomar medidas de seguridad para su conservación pudiendo copiarlos, e incluso incautarlos en situaciones graves con plazos acotados y regulados por la norma legal, así como requerir informaciones a terceros; con posibilidad, también, de acudir al auxilio de la fuerza pública y orden judicial de allanamiento.

CONSIDERANDO:

I- Que se trata de poderes-deberes concedidos a la Unidad para el ejercicio efectivo de sus cometidos de contralor, en aras de defender y preservar el interés público.

II- Que ello no inhibe de advertir, como es de orden en el Estado de Derecho, que tales facultades se deben utilizar aplicando juicios de razonabilidad y ponderación, procurando compatibilizarlas lo más posible con la vigencia y efectividad de otros Derechos Fundamentales.

III- Que el acceso y disponibilidad de datos de este tipo por parte de los funcionarios puede resultar esencial para la consecución de los fines perseguidos con la medida dispuesta, o bien puede no serlo.

IV- Que los criterios antes señalados, de razonabilidad y ponderación, determinan que solamente agotadas otras posibilidades (economía de medios), y siempre que estuviera en juego el propio éxito de la medida, se justifica avanzar hacia el conocimiento de la información sometida a secreto profesional.

V- Que por tanto, y dependiendo de las singularidades de cada caso, en aquellas labores fiscalizadoras e inspectivas donde resulte esencial conocer información sometida a secreto profesional, se atenderá a la economía de medios y a la actuación certera y objetiva como principios de actuación, sin perjuicio de poder requerir el levantamiento judicial del referido secreto.
VI- Que en todo caso se asegurará el derecho de defensa y contradictorio del sujeto inspeccionado o fiscalizado, y se buscará su máxima colaboración con las medidas dispuestas.

ATENTO:
A lo expuesto y a lo dispuesto por las normas legales citadas,
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:
Que en aquellas inspecciones y fiscalizaciones de bases de datos donde pudiera estar en juego la preservación del secreto profesional sobre ciertos datos, se actuará con razonabilidad y ponderación atendiendo las pautas establecidas en los Considerandos del presente Dictamen.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo
URCDP
m.b.

Dictamen N° 10 de 8 de julio de 2011.

Se dictamina sobre consulta de la Dirección Nacional de Medio Ambiente referida a entregar o no información relativa a plantas industriales.

DICTAMEN N°		EXPEDIENTE N°
10	2011	2011-2-10-0000016

Montevideo, 8 de julio de 2011.

VISTO:

La consulta realizada a la U.R.C.D.P., con vinculación a la negativa por parte de la Dirección Nacional de Medio Ambiente (DINAMA) de entregar los informes que las plantas industriales sitas en Montevideo deben entregar cuatrimestralmente a dicho organismo.

RESULTANDO:

I) Que con fecha 28 de agosto de 2009, la URCDP se pronunció en un caso similar mediante el Dictamen N° 9/2009.

II) Que con fecha 6 de abril del corriente, DINAMA se presenta, indicando que no entregaría los datos referidos a: nombre de la empresa, cantidad producida de todos los productos, consumo de agua, consumo de energía, personal empleado por turno, días trabajados, caudales de los efluentes líquidos, detalle de las muestras.

CONSIDERANDO:

I) Que la Ley Nº 18.331 en su artículo 17 establece que esta información, puede ser comunicada con el previo consentimiento informado del titular de los datos y mediante la acreditación de un interés legítimo que demuestre la necesidad de acceder a dicha información.

II) Que ante la falta del consentimiento, procede la disociación de los datos referidos a los nombres de las empresas que presentaron los informes.

ATENTO:

A lo precedentemente expuesto y a lo dispuesto por le Ley N° 18.331.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales.

DICTAMINA:

I. ESTABLECER QUE EN LA SITUACIÓN A QUE REFIEREN ESTOS OBRADOS PROCEDE LA ENTREGA DE TODOS LOS DATOS QUE SE SOLICITAN, DISOCIANDOSE LOS NOMBRES DE LAS PLANTAS INDUSTRIALES

EN EL CASO DE LOS REFERIDOS EN EL RESULTANDO II. II. VUELVAN ESTOS OBRADOS A LA U.A.I.P. Y PUBLÍQUESE.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
r.i.

Dictamen N° 11 de 20 de julio de 2011.

Se dictamina sobre consulta formulada por el Carrasco Lawn Tennis relativa a la procedencia de entregar copia del padrón social a pedido de los socios.

DICTAMEN N°		EXPEDIENTE N°
11	2011	193/2011

Montevideo, 19 de julio de 2011.

VISTO:

La consulta formulada por Carrasco Lawn Tennis Club (CLTC) acerca de si resulta ajustada a derecho la entrega de copias de su padrón social, a requerimiento de sus socios.

RESULTANDO:

I- CLTC aduce que las solicitudes de los socios responden a diferentes motivos, entre otros para ser utilizados en actos electorales internos de la Institución.
Afirma que en virtud de que el padrón social se conforma de sendos datos personales, a efectos de evitar abusos con los eventuales datos obtenidos se entendió no brindarlos sin el expreso consentimiento de los involucrados, en el marco de lo dispuesto por el artículo 72 de la Constitución de la República y de lo previsto por el artículo 9º de la Ley Nº 18.331.

II- Se expidió el informe jurídico N° 6090 de 20 de junio de 2011.

CONSIDERANDO:

I- Que la comunicación de datos que se pretende se encuentra regulada en el artículo 17 de la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP) y exige para su legitimidad la conjunción simultánea de los siguientes requisitos, el interés legítimo del emisor y del destinatario de la comunicación, y el previo consentimiento del titular de los datos, salvo las excepciones establecidas en la norma.
El interés legítimo solo podría verificarse desde la órbita del destinatario (socio de la Institución), pero no del emisor, que en principio no lo moviliza ningún interés ni simple ni cualificado.
La ausencia de este requisito, por sí solo bastaría para desestimar la comunicación de datos.

II- Que sin perjuicio de lo anterior, tampoco se configuran las excepciones enunciadas en el artículo 17 para validar la comunicación de datos sin el previo consentimiento del titular, habida cuenta de los principios generales que encauzan el tratamiento de los datos personales, especialmente el principio de finalidad regulado en el artículo 8º.

III- En efecto, salvo la hipótesis que en los estatutos o en la ficha de afiliación se detalle expresamente la posibilidad de comunicación de datos a otros socios, para finalidades específicas, deberá recabarse el

consentimiento informado del socio para legitimar la pretendida cesión de datos.
Tal consentimiento será inválido si la información que se facilita al titular no le permite conocer la finalidad a que se destinarán los datos comunicados o la actividad de la persona a la que se pretende comunicar, conforme lo dispuesto por el artículo 13 de la LPDP.

ATENTO:

A lo expuesto y a lo dispuesto por las normas legales citadas,
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Indicar que no procede comunicar datos personales de los socios, sin su consentimiento informado, salvo la hipótesis que dicho extremo resulte contemplado en los Estatutos del Carrasco Lawn Tennis o en la ficha de afiliación.
2) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.j.r.

Dictamen N° 11B de 20 de julio de 2011.

Se dictamina sobre consulta realizada por la Asesoría Jurídica de la Dirección Nacional de Asistencia y Seguridad Social Policial del Ministerio del Interior, respecto a la disponibilidad de datos personales en poder del Banco de Previsión Social.

DICTAMEN N°		EXPEDIENTE N°
11B	2011	2011-2-10-000072

Montevideo, 20 de julio de 2011.

VISTO:

La consulta proveniente de la Asesoría Jurídica de la Dirección Nacional de Asistencia y Seguridad Social Policial del Ministerio del Interior, respecto a la disponibilidad de datos personales en poder del Banco de Previsión Social.

RESULTANDO:

I.- Que la Dirección Nacional de Asistencia y Seguridad Social (D.N.A.S.S.P.) tiene los cometidos de dirigir, coordinar y supervisar las actividades de varios servicios, entre ellos el "Servicio de Retiros y Pensiones Policiales" y el "Servicio de Tutela Social Policial".

II.- Que desde su creación legal esta Dirección ha funcionado en coordinación con el Banco de Previsión Social, a través de un régimen de transición y suscribiendo Convenios interinstitucionales al efecto.

ATENTO:

A lo expuesto, al Informe Letrado Nº 6010/2011 de 9 de junio de 2011, y a lo dispuesto por los artículos 1º, 4º B), 9º inciso 3 literal B), 17 literal B) de la Ley N° 18.331, 157 a 160 de la Ley Nº 18.719.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

I) Establecer que:

1. La situación planteada refiere al intercambio de información entre organismos públicos, actividad que actualmente está regulada por los artículos 157 a 160 de la Ley Nº 18.719, de 27 de diciembre de 2010.
2. El intercambio de información y la interoperabilidad entre organismos públicos es de principio, por lo que debe primar un criterio básico de apertura y aceptación, con adecuación y respeto del derecho fundamental a la protección de datos personales.
3. En consecuencia, y en la medida que existan razones objetivas de servicio, procede actuar con arreglo al artículo 9º inciso 3º literal B), y al artículo 17 literal B) de la Ley Nº 18.331, de 11 de agosto de 2008, que permiten prescindir del consentimiento de los titulares de los datos para su registro y tratamientos,

incluyendo la comunicación de los mismos a la repartición de la que proviene la consulta.
4. A mayor abundamiento, las cláusulas 11 y 12 del "Convenio de Cooperación Interinstitucional para la Reingeniería de la D.N.A.S.S.P." agregado al expediente, han previsto y habilitan expresamente el referido intercambio, y su adecuación a la Ley Nº 18.331.
II) Notifíquese, publíquese y oportunamente archívese

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

Dictamen N° 12 de 29 de julio de 2011.

Se dictamina sobre la adopción de un nuevo plan de negocios de empresa que trata datos comerciales.

DICTAMEN N°		EXPEDIENTE N°
12	2011	3540/2010

Montevideo, 29 de julio de 2011.

VISTO:

Las aclaraciones presentadas por EQUIFAX URUGUAY S.A. (CDI) al Dictamen N° 26, de 17 de diciembre de 2010 que aprobó el nuevo esquema de negocio que la empresa pretende implementar, en sus implicancias con la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data (LPDP).

CONSIDERANDO:

I) Que la Unidad emitió el Dictamen Nº 26/2010, de 17 de diciembre de 2010 por el que entendió que el nuevo esquema de negocio en régimen de outsourcing que presentara la empresa, se adecua al régimen legal, bajo requisitos que releva el propio Dictamen y el cumplimiento de los principios contenidos en la Ley Nº 18.331 y su Decreto reglamentario Nº 414/009.

II) Que entre dichos principios figura el de finalidad previsto en el art. 8º de la Ley, exigible para la recolección y tratamiento de los datos.

ATENTO:

A lo expuesto, a los informes Nº 5089, de 7-IV-2011 y 6185, de 1-VII-2011, y a lo establecido en la normativa citada, El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Que complementando lo indicado por Dictamen Nº 26/2010, de 17 de diciembre de 2010, corresponde tener presente lo siguiente:

A) En todos los casos, el tratamiento de datos personales debe ostentar una finalidad legítima, la que podrá variar y concretarse con arreglo a los principios que surgen de la Ley Nº 18.331.

B) Cuando legalmente se exija el consentimiento del titular para la recolección o la comunicación ulterior de sus datos personales, todo cambio de finalidad no contemplado por las partes exigirá el consentimiento renovado del titular del dato.

2) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

Dictamen N° 13 de 9 de setiembre de 2011.

Se dictamina sobre consulta formulada por Obras Sanitarias del Estado (OSE) a efectos de adecuarse a las leyes de protección de datos y acceso a la información pública.

DICTAMEN N°		EXPEDIENTE N°
13	2011	171/2011

Montevideo, 9 de setiembre de 2011.

VISTO:

La consulta formulada por las Obras Sanitarias del Estado (O.S.E), a través del Sr. Enrique Balestrino, integrante de la comisión multidisciplinaria que pretende adecuar y alinear el Organismo a las Leyes Nos. 18.331 y 18.381, de Protección de Datos Personales y Acción de Habeas Data, y de Acceso a la Información Pública, respectivamente.

RESULTANDO:

I) Que el solicitante consulta si es válido el acceso del usuario de los servicios de agua potable y saneamiento a través del Portal de OSE, introduciendo su número de documento de identidad, cuando ese dato conduce a otros que pueden ser de índole privada.

II) Que se expidió el informe jurídico N° 5934, el 3 de junio de 2011.

CONSIDERANDO:

I) Que conforme lo dispuesto en el artículo 4°, literales D) y M) de la Ley Nº 18.331, de Protección de Datos Personales y Acción de Habeas Data (LPDP) que define dato personal y tratamiento de datos, respectivamente, y de acuerdo con lo previsto por los artículos 7º y 9º del mismo cuerpo normativo que regulan los principios de veracidad y previo consentimiento informado, no resulta recomendable la incorporación del dato personal cédula de identidad del usuario, en forma única, para acceder a la información que el Organismo brinda al usuario.

II) Que una persona que no sea el usuario consultante y que conozca el número de cédula de identidad de otra, podría acceder fácilmente a la factura del consultado, tomando conocimiento del nombre completo del titular del servicio, domicilio, tipo de tarifa de que se trata (familiar u otro), unidad, así como el detalle del consumo con el monto a pagar y deudas si las tuviere.

ATENTO:

A lo expuesto y lo dispuesto por las disposiciones legales citadas,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido que sería correcta la utilización del número de cédula de identidad, si en forma complementaria se incluye un password de carácter personal del usuario.
2) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.j.r.

Dictamen N° 14 de 15 de setiembre de 2011.

Se dictamina sobre consulta de la Dirección General de Casinos sobre videovigilancia en salas de juego.

DICTAMEN N°		EXPEDIENTE N°
14	2011	2011-2-10-000098

Montevideo, 15 de setiembre de 2011.

VISTO:

La consulta formulada por la Dirección General de Casinos referente a la videovigilancia en las diferentes Salas de Juego y aplicación de la normativa vigente en materia de protección de datos personales.

RESULTANDO:

I) Que el consultante pregunta si es correcto interpretar a los efectos de la inscripción, que el responsable de las bases del Organismo es el Director General de Casinos, aún cuando delegue en Gerentes de Salas o Casinos y en el Departamento de Circuitos Cerrados de Televisión.

II) Que asimismo requiere ser asesorado respecto a cómo garantizar el derecho de acceso a los interesados, sin exhibir la imagen de terceros que no han prestado su consentimiento, considerando el tipo de equipamiento y las limitaciones que posee el Departamento de Circuitos Cerrados de Televisión de la Dirección.

CONSIDERANDO:

I) Que el literal K) del artículo 4º de la Ley 18.331, dispone que el responsable de la base de datos o del tratamiento es la persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento, así como el art. 12 establece que por el Principio de Responsabilidad, el responsable de la base de datos será responsable de la violación de las disposiciones de la ley.

II) Que en la guía para el llenado de formularios de inscripción elaborada por la URCDP, se establece que se deberán indicar los datos del titular o representante de la Base de Datos o del tratamiento, y que el responsable es la 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 el caso de empresas privadas, se señalarán los datos del o los representantes estatutarios. En el caso de Organismos Públicos se detallarán los datos del Jerarca correspondiente.

III) Que de acuerdo al alcance de los términos responsable y encargado de tratamiento, así como de los cometidos específicos que posee la Dirección consultante, cabe concluir que el jerarca de la misma es quien debe representar a la Dirección General de Casinos, organismo obligado o responsable en los términos y alcance previstos en la norma, aunque delegue en diferentes encargados de tratamientos

según corresponda, ya sean Gerentes de Salas o Casinos, o en el Departamento de Circuitos Cerrados de Televisión.

IV) Que respecto al ejercicio del derecho de acceso, la URCDP se expidió mediante el Dictamen N° 10, de 16 de abril de 2010, estableciendo entre otras consideraciones, que a la videovigilancia es aplicable la normativa de protección de datos personales cuando se utilicen cámaras o cualquier otro medio análogo que capte, trate, registre o almacene imágenes que refieran a personas identificadas o identificables.

V) Que sin embargo, y tal como lo indica la Agencia Española de Protección de Datos (AEPD) en el Informe Jurídico 0193/2007, el acceso que se efectúe no puede implicar una violación a los derechos de terceros, por tanto el responsable deberá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento, con el objetivo de asegurar el equilibrio entre ambos derechos, esto es atender el acceso y no comunicar datos de terceros.

ATENTO:

A lo dispuesto por los arts. 4º literal K), 12, 14, 34 literal A) de la Ley Nº 18.331, de 11 de agosto de 2008;
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1.- La Dirección General de Casinos es el organismo público responsable de sus bases de datos de videovigilancia en los términos y alcance previstos en la Ley N° 18.331 y su Decreto reglamentario, y a efectos de la inscripción el Director de la Dirección General de Casinos es el jerarca que la representará, aunque en el cumplimiento de su cargo éste delegue en diferentes encargados de tratamientos según corresponda.

2.- A efectos de cumplir con la Ley se deberá garantizar el ejercicio del derecho de acceso (art. 14), dando respuesta por escrito a los solicitantes, dentro del plazo previsto en la Ley y detallando la información existente en la referida base sobre su persona, sin vulnerar derechos de terceros.

3.- Notifíquese, publíquese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
g.r.

Dictamen N° 15 de 15 de setiembre de 2011.

Se dictamina sobre consulta del Fondo de Solidaridad relativa a informar la identidad de los beneficiarios en su sitio web.

DICTAMEN N°		EXPEDIENTE N°
15	2011	2011-2-10-000180

Montevideo, 15 de setiembre de 2011.

VISTO:

La consulta formulada por el Fondo de Solidaridad (FDS) acerca de si se encuentra habilitado a informar la identidad de los beneficiarios de las becas que otorga la Institución y si la Universidad de la República (UdelaR) y UTU pueden proporcionarle los datos que permitan localizar a los egresados de dichos entes de enseñanza para la efectiva recaudación de los tributos.

RESULTANDO:

I- Respecto a la posibilidad de informar la identidad de los beneficiarios de las becas que otorga, el FDS indica que la situación le genera dudas, en tanto en el caso se contrapone el principio de transparencia de la gestión pública con el derecho a la protección de datos personales de los becarios.
En cuanto a la posibilidad de que la Universidad de la República y UTU proporcionen los datos de localización de los egresados señala que existen razones de hecho y fundamentos de derecho que legitimarían la comunicación de datos que se pretende.

II- Se expidió el informe jurídico N° 6039, de 13 de junio de 2011.

CONSIDERANDO:

I- Que el artículo 9º de la Ley Nº 16.524 impone a la UdelaR y a la UTU, el envío a la Comisión del FDS, de la nómina completa de quienes hayan obtenido títulos profesionales comprendidos en la ley durante el año inmediato anterior y la fecha exacta de expedición. Asimismo, exige que la UdelaR proporcione a la Comisión del FDS, la información registrada en el Servicio Central de Bienestar Universitario, a fin de coordinar el cumplimiento de la Ley.

II- Que conforme lo anterior y lo dispuesto por el artículo 17, 9º literal B) y 7º de la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP) que regulan la comunicación de datos, la excepción de recabar el consentimiento del titular cuando medie una Ley, y el principio de veracidad, respectivamente, resulta pertinente de acuerdo con el principio de finalidad, que la UdelaR y la UTU comuniquen al FDS además de los nombres y apellidos de egresados, fechas de egreso y carreras asociadas, el domicilio de aquéllos. Todo ello en atención a las disposiciones legales citadas, que se complementan con lo previsto por el literal C) del artículo 9º de la LPDP que contempla al domicilio como un dato que no requiere el consentimiento del titular para su tratamiento y/o comunicación.

III- Que en relación con la posibilidad de informar la identidad de los beneficiarios de las becas que el FDS concede, realizando una ponderación de los derechos en juego -protección de datos personales y acceso a la información pública- y habida cuenta de las previsiones contenidas en los artículos 8º y 17 literal D) de la LPDP que regulan el principio de finalidad y la comunicación de datos, respectivamente, procede la divulgación de información de los becarios a la cual se le aplique un procedimiento de disociación, de modo que los titulares de los datos no sean identificables.

ATENTO:

A lo expuesto y a lo dispuesto por las normas legales citadas,
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Expedirse en el sentido de que conforme las disposiciones de la LPDP analizadas a la luz de los cometidos asignados por Ley al Fondo de Solidaridad, la Universidad de la República y la ANEP- Consejo de Educación Técnico Profesional (UTU) están habilitados a comunicarle los domicilios de sus egresados, además de la respectiva nómina fecha de egreso y carrera asociada.

2) En cuanto a la posibilidad de informar la identidad de los becarios, procede la divulgación de información, disociada de los titulares, al amparo de lo previsto por el literal D) del artículo 17 de la LPDP.

3) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.j.r.

Dictamen N° 16 de 14 de octubre de 2011.

Se dictamina sobre consulta relativa a la posibilidad de realizar transferencias internacionales de datos.

DICTAMEN N°		EXPEDIENTE N°
16	2011	2011-2-10-0000594

Montevideo, 14 de octubre de 2011.

VISTO:

La consulta presentada por Royal & SunAlliance Seguros (Uruguay) S.A.

RESULTANDO:

I. Que la consulta refiere a la legalidad de transferir datos a Argentina a los efectos de realizar una encuesta a los corredores que trabajan para la empresa.

II. Que la base de datos de corredores de RSA se encuentra en proceso de inscripción.

III. Que la consulta pasó a informe jurídico el viernes 16 de setiembre del corriente año, realizándose éste con fecha 20 de setiembre del mismo año.

CONSIDERANDO:

I. Que resulta aplicable la Ley N° 18.331, de 11 de agosto de 2008, por tratarse de información contenida en una base de datos personales.

II. Que según la Ley, transferencia internacional de datos es aquel tratamiento 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.

III. Que conforme el artículo 23 de la Ley se prohíbe la transferencia internacional de datos a aquellos países que no sean adecuados.

IV. Que de acuerdo con la Resolución N° 17, de 12 de junio de 2009, del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, se consideran apropiados para la transferencia internacional de datos aquellos países que cuenten con normas de protección de datos adecuados y medios para asegurar su aplicación eficaz. Y, que entre ellos, se encuentran comprendidos los países que la Comisión Europea considera que garantizan las condiciones indicadas.

V. Que Argentina, conforme con la Decisión 2003/490/CE de la Comisión Europea, se considera un país adecuado.

VI. Que la presente consulta indica que se transferirán los datos a Argentina para su tratamiento, por lo que

la transferencia de datos se considera conforme con la Ley.

VII. Que se debe informar en la solicitud de inscripción de base de datos de corredores que se realizará una transferencia internacional de datos, el destino, el tipo de datos y la finalidad.

VIII. Que se debe dar cumplimiento al resto de la normativa de la protección de datos.

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:

I. Podrán transferirse datos personales a Argentina por poseer declaración de país adecuado.

II. Deberá informarse que se va a realizar una transferencia internacional de datos en la solicitud correspondiente de inscripción de base de datos conforme lo expuesto en el Considerando VII.

III. Deberá darse cumplimiento a todos los principios consagrados en la Ley.

IV. Notifíquese, y oportunamente publíquese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
f.b.

Dictamen N° 17 de 14 de octubre de 2011.

Se dictamina sobre consulta de la Caja Notarial relativa a nota pidiendo información relacionada con el Sistema Notarial de Salud.

DICTAMEN N°		EXPEDIENTE N°
17	2011	2011-2-10-000433

Montevideo, 14 de octubre de 2011.

VISTO:

La consulta presentada por el Directorio Honorario de la Caja Notarial para que se emita opinión sobre el contenido de su Resolución Nº 1813, adoptada en sesión del 10 de mayo de 2011.

RESULTANDO:

I.- Que en el citado acto, el consultante resolvió acerca de una petición que contiene un conjunto de pedidos de información, presentado por dos asociados, y avalados posteriormente por la Asamblea Nacional de Escribanos.

II.- Que el pronunciamiento se fundó en informe de su Asesor Letrado, haciendo lugar a alguno de los pedidos y rechazando otros, esto último en función de diversos criterios según el tipo de información solicitada.

III.- Que alguno de los pedidos, no todos, fueron rechazados por entender la consultante que se trata de datos personales cuya comunicación requiere consentimiento de sus titulares.

CONSIDERANDO:

I.- Que la Unidad actúa, como todo órgano estatal, bajo la égida del principio de especialidad, por lo que solamente le compete pronunciarse acerca de cuestiones que involucren el régimen jurídico de la protección de datos personales. (cf. Risso Ferrand, Derecho Constitucional t. III, pág. 70 y ss., ed. Ingranusi, 1998).

II.- Que el Consejo acompaña el estudio y fundamentos sobre los veinte (20) ítems que integran el asunto consultado, expuestos en el Informe Letrado Nº 6548/2010 emitido en este expediente, por lo que en base a razones de brevedad se hará remisión al contenido de dicho Informe Letrado, considerándolo integrado al presente Dictamen.

ATENTO:

A lo expuesto, al Informe Letrado Nº 6548/2011, de 26-VIII-2011, y a lo dispuesto por los artículos 9º, 17 y 34 lit. F). de la Ley Nº 18.331,

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

I) Dar respuesta a la consulta formulada, en los términos que surgen del Informe Letrado Nº 6548/2011, de fecha 26-VIII-2011 emitido en esta Unidad, cuyo contenido será copiado y pasará a formar parte del presente Dictamen en forma de "Anexo".

II) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

ANEXO

Informe Nº 6548/2011 Exp. Nº 2011-2-10-0000433: Consulta Caja Notarial

I. Planteo

Se solicita un pronunciamiento de la Unidad, respecto a la Resolución del Directorio Honorario Nº 1813 de la Caja Notarial, adoptada en su sesión de 10 de mayo.

Según los antecedentes que acompañan la consulta, el contenido de la mencionada Resolución refiere un acogimiento parcial por parte del Directorio, a una serie de petitorios expuestos en una Nota presentada por dos asociados, que luego fuera avalada por la Asamblea Nacional de Escribanos.

En dicha Nota se solicita un cúmulo de informaciones relacionados con el Sistema Notarial de Salud.

El pronunciamiento recaído y sometido a consulta está fundado en opinión letrada emitida previamente a requerimiento del Directorio de la consultante, del que surge que algunas de las informaciones solicitadas constituyen "datos personales" de terceros, que no cuentan con el requisito de consentimiento de los afectados para ser comunicados, y en base a ello se deniega su libramiento.

En el mismo pronunciamiento, siguiendo la opinión letrada previa y respondiendo a alguno de los ítemes peticionados, se apela a fundamentos ajenos a la protección de datos personales, para autorizar o rechazar su comunicación.

De acuerdo al principio de especialidad que fija los márgenes de actuación y pronunciamiento de todo órgano estatal (cf. Risso Ferrand, Derecho Constitucional t.III, p. 70 y ss., ed. Ingranusi, 1998), el presente Informe se abocará a analizar exclusivamente aquéllos contenidos de la Resolución, y la Nota a que remite, que presentan una relación directa con el régimen jurídico de protección de datos personales, consagrado mayormente por el art. 72 de la Constitución de la República, la Ley Nº 18.331 de 11-08-2008, su modificativa Ley Nº 18.719 de 27-12-2010, y el Decreto Reglamentario Nº 664/008 de 22-12-2008.

II. Análisis general

La protección jurídica de los datos personales conforma un sistema normativo hasta cierto punto novedoso en el derecho nacional, cuya vigencia efectiva en los distintos ámbitos de la sociedad depende, en última instancia, de su correcto entendimiento, para poder así cumplir cabalmente con una serie de reglas de derecho que emanan del régimen.

Estas reglas no son otra cosa que la traducción o pasaje a derecho positivo de un conjunto armonioso de principios generales, derechos y obligaciones, mayormente presentes o derivados de las normas citadas en el apartado I. Pero justo es advertir que si estas normas de derecho positivo no existieran, igualmente el régimen estaría operante en sus lineamientos esenciales, por virtud que se trata de un derecho fundamental con asiento en el art 72 de la Constitución de la República, que no requiere reglamentación para su vigencia conforme lo señala el art. 332 del mismo cuerpo.

O sea que por encima de otro tipo de consideraciones igualmente presentes y válidas pero de naturaleza consecuente, debe partirse de esta primera apreciación: la protección de datos personales es un derecho fundamental de base constitucional, reconocido por nuestro orden jurídico, y de obligatorio respeto.

Remitiéndonos al caso en consulta, surge como apreciación liminar que el petitorio presentado a la Caja Notarial por los asociados movilizó incuestionablemente ciertos aspectos del régimen objeto de regulación y control por parte de la URCDP. Tales aspectos remiten a los "derechos referentes a la comunicación de datos" (art. 17 LPDP).

Vale decir que la hipótesis convocada en el contenido de la petición, fue aquélla que refiere a datos personales recolectados originalmente por un sujeto de derecho, a cuyo conocimiento aspiran otros sujetos de derecho, diferentes al que los recabara. Esta es la tipificación del caso en consulta. Al análisis en concreto de ello habremos de abocarnos en el presente Informe.

La "comunicación de datos personales" está definida por la propia LPDP como "toda revelación de datos realizada a una persona distinta del titular de los datos" (art. 4 lit. B LPDP). Coincide, pues, con el objetivo perseguido por los peticionantes al formular su solicitud.

Ahora bien, la regla a seguir tanto para la recolección como para la comunicación de datos personales, es la de obtener el consentimiento del titular afectado. Un consentimiento que, por ley, debe ser "libre, previo, expreso, informado, el que deberá documentarse" (arts. 9 y 17 de la LPDP). Esta regla admite excepciones, que las aludidas normas también prevén, y son las siguientes:

- datos provenientes de fuentes públicas de información;
- datos recabados para funciones propias de poderes del Estado o en virtud de obligación legal;
- datos meramente identificatorios cuyas especies define la propia ley;
- datos derivados de relación contractual, científica o profesional y necesarios para su desarrollo y cumplimiento;
- datos de uso exclusivo, individual o doméstico;
- cuando así lo disponga una ley de interés general;
- comunicación de datos de salud, cuando existan razones sanitarias, de emergencia, o realización de estudios epidemiológicos, preservando la identidad de los titulares por mecanismos de disociación cuando ello sea pertinente.
- datos disociados de sus titulares.

Siendo éste el régimen aplicable al caso en consulta, debemos pasar a determinar si el Directorio de la Caja Notarial dictó una Resolución ajustada a derecho, cuando accedió a algunos petitorios de comunicación de datos y desechó otros, según se considerase autorizado o inhibido para dicha comunicación. Procede, entonces, emitir nuestra opinión al respecto.

III. Nuestra opinión

Bajo los preanotandos expuestos, corresponde informar lo que sigue:1

1. "Dictamen de Jurídica de la Caja".- No se conoce el contenido de este documento, por lo que no resulta posible emitir una opinión concluyente al respecto. Tampoco existe una definición jurídica unívoca y obligatoria de lo que configura genéricamente un "dictamen", lo cual acrecienta las posibles dudas.

Es evidente, sin embargo, que quienes conocen el contenido del concreto documento solicitado, han entendido que se trata de información pública. Por lo tanto habrá de estarse a dicha evaluación. No obstante

ello, se advierte que si el Dictamen de marras contuviera datos personales, en grado tal de comprometer la privacidad de personas físicas o incluso jurídicas, la comunicación a terceros debería hacerse con arreglo a soluciones contemporizadores que sacrifiquen lo menos posible ambos derechos en colisión, el de acceso a la información pública y el de protección de los datos personales. Una solución recurrente a tales fines es producir lo que se conoce como "versión pública" del texto en cuestión, facilitando de este modo la entrega de las piezas requeridas, pero ocultando las informaciones nominativas que contengan.

2. "Informe IV realizado para el MTSS".- Merece consideraciones similares a las realizadas en numeral anterior.

1 Se sigue la misma numeración de la petición presentada a la Caja Notarial, fs. 3 y ss.

3. "Acta de la Comisión de Salud del Senado, integrada con Hacienda".-Merece consideraciones similares a las realizadas en numeral 1.

4. "Boletín "De Primera Mano".- A los efectos de la LPDP se trata de una "fuente pública de información", como tal factible de comunicación a terceros sin necesidad de contar con el consentimiento previo de los afectados (arts. 9 lit. A y 17 lit. B LPDP). Por tanto, la Resolución en consulta es correcta.

5. "Lista completa de los Afiliados a la Caja Notarial".- Se trata de datos personales que no están excluidos del requisito de consentimiento, máxime cuando se solicitan bajo un conjunto de criterios diferenciales que aleja definitivamente toda posibilidad (en cualquier caso no concluyente) de aplicar al punto la excepción del art. 9 lit. C de la LPDP. Es correcta, por tanto, la postura adoptada por la Resolución en este punto.

6. "Obtener del Hospital Británico, y si es posible también de los médicos de Policlínica, informes escritos -sin identificar a las personas- que contengan datos sobre porcentajes de...".- Desde el ángulo que compete la actuación de la URCDP no habría problemas en presentar esta información disociada, si la Caja dispusiera de ella. No obstante ello, la Resolución en consulta apela a otro tipo de motivaciones para fundar la denegatoria, sobre las que no corresponde pronunciarse.

7. "Reglamento o Estatuto que rige el Sistema Notarial de Salud".- Se trata de un tipo de información que, por su generalidad y abstracción, no entra en relación con el régimen de la protección de datos personales, siendo correcta la postura adoptada por la Resolución en tal sentido.

8. "Contratos celebrados con el Hospital Británico".- Partimos de la base que en estos contratos no figuran más datos personales que los pertenecientes a la Caja Notarial y a la institución médica nombrada. Al contrario de la postura seguida por la Caja Notarial, se entiende que esos datos son los que habitualmente se conocen como meramente identificatorios, cuyo tratamiento sin consentimiento de sus titulares está legalmente autorizado (art. 9 lit. C de la LPDP). Si así no fuera, igualmente y del punto de vista de la protección de datos personales, cabría apelar al criterio de liberar una versión pública, conforme lo expresado

para el ítem 1. En definitiva, y hasta donde se puede opinar sin haber tenido conocimiento del contenido concreto de estos contratos, todo hace pensar que se trata de un tipo de información que, por generalidad y trascendencia, debería calificarse como pública. En tal sentido, prima a juicio de este informante el criterio de su acceso, no así la postura denegatoria dictada por el órgano peticionado y consultante en este punto.

9. "Descripción de los Servicios que presta el Sistema Notarial de Salud a través de...".- Se trata de un ítem que puede revestir mayor grado de dificultad que los anteriormente comentados, a la hora de arribar a una definitoria postura al respecto. Reconociendo lo opinable del tema, y ateniéndonos exclusivamente a un enfoque centrado en el régimen objeto de competencia de la URCDP, la conclusión a adoptar por el suscrito informante es contraria a la postura sustentada en la Resolución.

La información requerida en estos casos no compromete mayormente el régimen de la protección de datos personales. Las razones para concluir así son las siguientes: Véase en primer lugar que se alude, en forma general, a un "Sistema Notarial de Salud", lo que determina un grado de abstracción mucho más proclive a facilitar la transparencia y publicidad de las informaciones que componen tal sistema, de interés para el conocimiento de un cúmulo de personas físicas (los asociados al sistema), y la sociedad en general.

Por otra parte, la información pretendida no parece apuntar a traslucir ningún dato nominativo perteneciente a los usuarios del sistema, sino más bien cuestiones disociadas de toda titularidad salvo la del Hospital (número de médicos, costos, montos...). No es intrascendente, a la hora de evaluar el punto, que el órgano peticionado sea nada menos que uno de los interlocutores principales y protagonistas del aludido Sistema Notarial de Salud, que en caso de detentar este tipo de informaciones lo hace siempre en aras de un interés común, al servicio de su masa de asociados. En tales circunstancias, negar el acceso o comunicación al abrigo de otras razones, no parece ser la mejor solución.
El derecho a la protección de datos personales si bien aplicable a las personas jurídicas (para el caso el Hospital Británico), de todos modos lo es "por extensión" y "en cuanto corresponda" (art. 2 LPDP), lo cual deja margen como para opinar en favor de la apertura informativa según el tipo de información requerida. En opinión del suscrito, y atendiendo a las características de la información solicitada y los sujetos que las detentan, debe primar la publicidad, por sobre la reserva, salvo que hubiera cláusulas contractuales de confidencialidad que impidieran lo primero. No siendo así, y en la medida que disponga de ella (que no está dicho que ocurra para todos los literales del ítem 9 expresados en la petición), la Caja Notarial parece ser el ámbito adecuado para brindar las informaciones consignadas.

10. "Informe del Hospital Británico en que describa la tecnología y servicios especiales que presta...".- Estrictamente no se trata de un pedido de "comunicación de datos personales" dirigido a quien dispone de ellos, por lo que no corresponde pronunciamiento al respecto.

11. "Los Medicamentos que se ordenan desde la Policlínica... del H. Británico".- El petitorio en este punto (desbrozado en tres literales) no tiene relación, en principio, con el régimen de protección de datos

personales. Sin perjuicio de ello, se formula la reserva sobre el alcance del literal c), en la medida que alude a "casos especiales..." Si éstos refirieran a "personas físicas o jurídica determinadas o determinables" (art. 4 lit. D de la LPDP), no corresponde franquear el acceso peticionado sin antes recabar el consentimiento de estas personas. En cambio, si la misma expresión es tan solo un giro de léxico para referir a un conjunto de situaciones genéricas sin personalización alguna, el acceso no compromete el régimen objeto de tutela.

12. "¿Existe algún reglamento o acuerdo del SNS con el Hospital Británico y la Policlínica en referencia al tiempo de espera para consultas generales o con especialistas?" Nos merece el mismo criterio explicitado con respecto al ítem Nº 9, al que nos remitimos.

13. "Información escrita sobre: a) Distribución del trabajo entre los escribanos activos. b) Ingresos promedio dentro de cada escala de activos. c) Montos de las pasividades y porcentajes de distribución."- La Resolución en consulta aprueba en su totalidad esta comunicación. A nosotros nos queda la duda, mayormente sobre el literal a), pero posiblemente por falta de información. Si refiere a información de tipo estadístico (lo que es presumible), estamos ante datos disociados y su comunicación no presenta problemas para el régimen (art. 17 lit. D de la LPDP).

14. "Monto total que: Recibe hoy el Fondo Sistema Notarial de Salud...".-Su comunicación no plantea objeciones para la consultante, y tampoco para nosotros.

15. Quienes fueron los delegados desde el 2009 hasta la fecha, en las gestiones de modificación de la Ley 18.211.- Merece igual opinión que el ítem precedente.

16. "Convoque a los afiliados para que, aquellos que lo deseen, consientan en ser identificados, y estén de acuerdo, presten testimonio ante Escribano Público, sobre...".- Nos remitimos a la solución informada para el ítem 10.

17. "Solicite al Hospital Británico un informe recabado de los médicos, que indique:...".- Igual criterio que el ítem anterior.

18. "Términos del nuevo acuerdo con el Hospital Británico, con especial claridad en cuanto:...".- Nos remitimos a la solución de los ítemes 8 y 9.

19. "Solicite al Instituto Nacional de Estadísticas...".- Nos remitimos a la solución informada para el ítem 10.

20. "Finalmente: pedimos ser recibidos por el Directorio de la Caja Notarial".- No corresponde pronunciarse.

IV. Conclusiones

1.- Compartimos parcialmente lo resuelto por la Caja Notarial, de acuerdo a fundamentos que en algunos casos se pliegan totalmente a la denegatoria operada, mientras que en otros ello no ocurre o se entiende que hay matices al respecto.

2.- Con arreglo al "principio de especialidad" que preside la actuación de la URCDP en tanto órgano público estatal, nos hemos limitado a analizar e informar exclusivamente respecto de una adecuación al régimen de competencia propio de la Unidad.

3.- Por lo tanto se dejaron a un lado otro tipo de fundamentos validantes o invalidantes de la comunicación requerida por las asociadas, que en varios casos manejaron el letrado pre opinante y la Resolución en examen. Ello no supone ni restar ni sumar importancia a esta otra clase de argumentos, cuando se dieron.

4.- En definitiva, la relación fundada expuesta en el apartado precedente, ítem por ítem, refleja nuestra postura sobre la adecuación del pedido de información elevado por los asociadas, según el tipo de informaciones requeridas en cada ítem.

Dr. Marcelo Bauzá
Derechos Ciudadanos

Dictamen N° 18 de 14 de octubre de 2011.

Se dictamina sobre consulta del Ministerio de Ganadería, Agricultura y Pesca acerca de la posibilidad de comunicar datos al Ministerio del Interior.

DICTAMEN N°		EXPEDIENTE N°
18	2011	2011-2-10-000587

.

Montevideo, 14 de octubre de 2011.

VISTO:

La consulta presentada por el Ministerio de Ganadería, Agricultura y Pesca y el Ministerio del Interior.

RESULTANDO:

I. Que la consulta refiere a la posibilidad de que el Ministerio de Ganadería, Agricultura y Pesca comunique datos al Ministerio del Interior en el marco del proyecto presentado como Fondo Concursable de AGESIC denominado “Fortalecimiento de la Seguridad del Movimiento de Semovientes”.

II. Que el Ministerio de Ganadería, Agricultura y Pesca trasferiría los siguientes datos al Ministerio del Interior: número de DICOSE, número de caravana, número de padrón de campo, cédula de identidad del propietario (eventualmente puede requerirse también el nombre), identificación de la marca y razón social.

III. Que el expediente pasó a informe jurídico, el cual se realizó con fecha 19 de setiembre de 2010.

CONSIDERANDO:

I. Que estamos ante la presencia de datos personales, algunos determinados como el nombre, la cédula de identidad, el RUT, y otros determinables, por lo que es aplicable al caso concreto la LPDP.

II. Que la consulta presentada refiere a una comunicación de datos entre el Ministerio de Ganadería, Agricultura y Pesca y el Ministerio del Interior.

III. Que según el artículo 17 de la LPDP, los datos personales objeto de tratamiento 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 debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.

IV. Que en el caso de marras sería aplicable la excepción relativa a que no es necesario recabar el consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del

Estado o en virtud de una obligación legal, la cual es aplicable por la remisión que hace el literal B) del artículo 17 de la LPDP.

V. Que el Sistema Nacional de Información Ganadera (SNIG) es un sistema de información que tiene como objetivo principal asegurar la trazabilidad del ganado vacuno desde el establecimiento de origen del animal hasta el frigorífico, tanto individualmente como por grupos de animales, de acuerdo con las disposiciones y reglamentaciones del MGAP

VI. Que el Ministerio del Interior tiene como cometido asegurar la seguridad nacional y para ello debe prevenir y combatir el delito.

VII. Que en la presente consulta se verifica la excepción contenida en el artículo 9° literal B) de la Ley, por lo que la comunicación de datos es legítima ya que el Ministerio del Interior está ejerciendo funciones propias del organismo y los datos provienen de otro organismo, por lo que no sería necesario recabar el consentimiento de los titulares.

VIII. Que igualmente se hace aplicable el resto de la normativa vigente, sobre todo los principios que regulan la protección de datos.

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:

I - Establecer que es legítima la comunicación de datos entre el Ministerio de Ganadería, Agricultura y Pesca y el Ministerio del Interior.

II- Indicar que no es necesario recabar el consentimiento de los titulares porque se verifica la excepción relativa al ejercicio de las funciones propias de los organismos.

III. Recomendar que se apliquen las demás disposiciones relativas a la protección de datos.

IV. Notifíquese, y oportunamente publíquese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

f.b.

Dictamen N° 19 de 21 de octubre de 2011.

Se dictamina sobre consulta de la Intendencia de Rivera sobre la posibilidad de publicar ciertos datos en sus servicios en línea.

DICTAMEN N°		EXPEDIENTE N°
19	2011	2011-2-10-000448

Montevideo, 21 de octubre de 2011.

VISTO:

La consulta realizada por la Intendencia de Rivera sobre la posibilidad de publicar ciertos datos en los servicios de consulta de deuda e impresión de factura.

RESULTANDO:

Que con fecha 11 de febrero de 2010, la URCDP se pronuncia en un caso similar, "Que de acuerdo con el principio de finalidad consignado en el artículo 8° de la LPDP, los datos personales no deben utilizarse para una finalidad distinta para la que fueron recabados, en el caso de marras, no sería necesario consignar el nombre de la persona para cumplir con la finalidad buscada…"

CONSIDERANDO:

I) Que de acuerdo al artículo 8° de la citada Ley N° 18.331, no se deberían incluir en la factura web los datos adicionales del padrón, nombre y RUC del propietario, nombre y RUC del contribuyente, dirección y teléfono del contribuyente y datos "información al contribuyente"; dado que no son necesarios para la finalidad consulta de deuda e impresión de factura.

II) Que no corresponde a la URCDP pronunciarse sobre: si se debe solicitar al usuario el número de padrón o el código interno del padrón para acceder a la información; si el usuario debe seleccionar parte de la deuda vencida, toda la deuda vencida o las cuotas a vencer a fin de generar la factura para impresión.

ATENTO:

A lo precedentemente expuesto y a lo dispuesto por la Ley N° 18.331.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales.

DICTAMINA:

I. RECOMENDAR A LA INTENDENCIA DE RIVERA PARA LOS SERVICIOS DE CONSULTA DE DEUDA E IMPRESIÓN DE FACTURA A TRAVÉS DE SU PÁGINA WEB ELIMINAR EL DATO NOMBRE DEL PROPIETARIO Y NO CONSIGNAR LOS DATOS RESEÑADOS EN EL CONSIDERANDO I).

II. SEÑALAR A LA CITADA INTENDENCIA TENGA PRESENTE LA CLAÚSULA DE CONSENTIMIENTO PARA

EL CASO DE QUE NO SEAN DATOS REQUERIDOS PARA LA FUNCIÓN PROPIA DEL ORGANISMO.

III. NOTIFÍQUESE Y PUBLÍQUESE.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
r.i.

Dictamen N° 20 de 21 de octubre de 2011.

Se dictamina sobre la consulta formulada por la Asociación Uruguaya de Empresas Aseguradoras acerca de la posibilidad de implementar una base de datos de seguros.

DICTAMEN N°		EXPEDIENTE N°
20	2011	2011-2-10-000517

Montevideo, 21 de octubre de 2011.

VISTO:

La consulta formulada por la Asociación Uruguaya de Empresas Aseguradoras (AUDEA) acerca de la implementación de una base de datos denominada Base de Datos de Seguros.

RESULTANDO:

I) Que la consultante expresa que dicha base sería el resultado de un proyecto desarrollado y promovido por el sector asegurador privado nucleado en la AUDEA, teniendo como objetivo central la prevención y combate del fraude en los seguros.

II) Que sus características principales serían las siguientes: 1) A su contenido sólo podrán acceder las empresas que forman parte de la AUDEA, 2) El encargado de tratamiento será EQUIFAX URUGUAY S.A., en tanto que la AUDEA será la responsable de la misma y 3) Sólo se registrarán los datos referidos al historial de siniestros e incumplimientos en seguros generales y SOA, no incluyéndose dentro de la misma datos sensibles, por lo que se exceptúan del registro los seguros de salud de las personas.

CONSIDERANDO:

I) Que como las aseguradoras privadas deberán comunicar los datos de sus clientes a efectos de su conformación, corresponde analizar su creación a la luz principalmente de los arts. 8°, 9° y 17 de la Ley N° 18.331.

II) Que si bien el art. 9° establece una serie de excepciones que eximen al responsable de una base de datos de su obligación de recabar el consentimiento del titular para poder comunicar los datos a un tercero, las mismas no aplican al caso en cuestión.

III) Que en el caso de España por ejemplo, la formación de este tipo de base de datos por parte de las aseguradoras privadas está autorizada expresamente por ley, pero ello no es así en nuestro país, por ende no es de aplicación el art. 9° B) de la Ley N° 18.331.

IV) Que en definitiva tal como indica el artículo 17 de la Ley, para que las aseguradoras privadas comuniquen los datos de sus asegurados a efectos de formar la base, cada una deberá recabar el consentimiento e informar al titular sobre la finalidad de tal comunicación y de la existencia de la base, así como brindar la

información relacionada con el encargado de tratamiento y las formas en que podrán ejercer los derechos consagrados en la Ley.

V) Que a su vez, la base deberá ajustarse a las características que se informan en la consulta, sobre todo en lo que respecta a su contenido y a la finalidad. Cualquier cambio deberá ser comunicado oportunamente a la URCDP (art. 20, Decreto 414/009).

VI) Que asimismo corresponde que la base sea debidamente inscripta en el Registro de la URCDP y que se adopten las medidas de seguridad recomendadas a efectos de que se ajuste a lo dispuesto en el art. 10 de la Ley.

ATENTO:

A lo dispuesto por los arts. 6°, 8°, 9°, 10, 12, 13, 17, 34 lit A) de la Ley Nº 18.331, de 11 de agosto de 2008;

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1.- Que para la conformación de la referida base de datos, cada aseguradora que comunique estos datos a la AUDEA, deberá recabar el consentimiento e informar al titular sobre la finalidad de tal comunicación y de la existencia de dicha base.

2.- A efectos de cumplir con la ley también deberá inscribirse la misma, ajustarse a las características que se informan en la consulta, sobre todo en lo que respecta al contenido y finalidad, así como adoptar medidas de seguridad acordes.

3.- Notifíquese, publíquese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
g.r.

Dictamen N° 21 de 21 de octubre de 2011.

Se dictamina sobre consulta de la Junta Nacional de Drogas referente a la posibilidad de crear una base de datos de usuarios.

DICTAMEN N°		EXPEDIENTE N°
21	2011	2011-2-10-000584

Montevideo, 21 de octubre de 2011.

VISTO:

La consulta realizada por la Junta Nacional de Drogas (JND) sobre la posibilidad de crear una base de datos con los usuarios en centros de tratamiento.

RESULTANDO:

Que por informe jurídico de fecha 16 de setiembre se recomienda a la JND la consideración de los principios legales en el tratamiento de datos especialmente protegidos. Asimismo por informe técnico se recomiendan una serie de medidas de seguridad a implementar.

CONSIDERANDO:

I) Que de acuerdo al artículo 9° de la Ley N° 18.331, no sería necesario el previo consentimiento informado, ya que se trata del ejercicio de una obligación legal.

II) Que de acuerdo al Decreto N° 414/009, la base de datos creada debe ser inscripta ante la URCDP.

ATENTO:

A lo precedentemente expuesto y a lo dispuesto por la Ley N° 18.331.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales.

DICTAMINA:

I. RECOMENDAR A LA JUNTA NACIONAL DE DROGAS TOMAR EN CONSIDERACIÓN LOS PRINCIPIOS DE LEGALIDAD, VERACIDAD, FINALIDAD, SEGURIDAD, RESERVA Y RESPONSABILIDAD DE LA LEY N° 18.331, ASÍ COMO LA IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD RESEÑADAS EN EL INFORME TÉCNICO.

II. INDICAR A LA JUNTA NACIONAL DE DROGAS LA INSCRIPCIÓN DE LA BASE DE DATOS CREADA, DE ACUERDO AL DECRETO N° 414/009.

III. NOTIFÍQUESE Y PUBLÍQUESE.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
r.i.

Dictamen N° 22 de 21 de octubre de 2011.

Se dictamina sobre consulta de Secretaría General de AGESIC respecto de la adecuación a la normativa legal vigente para solicitar datos personales a los funcionarios.

DICTAMEN N°		EXPEDIENTE N°
22	2011	2011-2-10-000602

Montevideo, 21 de octubre de 2011.

VISTO:

La consulta presentada por la Dra. Suevia Sánchez de la Secretaría General de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC).

RESULTANDO:

I. Que la consulta refiere a la adecuación de los datos personales que se solicitará informen los funcionarios de AGESIC en el marco de las relaciones de trabajo que los vinculan.

II. Que los datos solicitados los incorporarán los funcionarios a una "Ficha Personal" y serán gestionados por el Grupo de Gestión Humana de AGESIC.

III. Que la consulta pasó a informe jurídico con fecha 22 de setiembre de 2011.

CONSIDERANDO:

I. Que resulta aplicable la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP) por tratarse de datos personales conforme con la definición del artículo 4° literal d) de la Ley.

II. Que los datos requeridos se refieren a datos identificatorios, grupo familiar, datos de salud, calificación personal, datos laborales y medio de transporte utilizado para llegar al trabajo.

III. Que se constata el cumplimiento del principio de veracidad de los datos, en tanto, se entiende que los datos son los necesarios para el tratamiento a realizarse.

IV. Que en lo que respecta a los datos de salud, se recomienda que se adopten medidas de seguridad suficientes para resguardar su confidencialidad.

V. Que en el tratamiento que se realice de estos datos personales es necesario aplicar el resto de los principios y derechos regulados en la Ley.

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:

I- Indicar que los datos requeridos son los adecuados para la finalidad para la cual se pretenden recabar.

II- Recomendar que se adopten las medidas necesarias para garantizar el cumplimiento de los principios y derechos que consagra la Ley.

IV. Notifíquese, y oportunamente publíquese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

f.b.

Dictamen N° 23 de 28 de octubre de 2011.

Se dictamina sobre una consulta de Obras Sanitarias del Estado (OSE) en relación con el tratamiento de datos de salud del personal.

DICTAMEN N°		EXPEDIENTE N°
23	2011	2011-2-10-000603

Montevideo, 28 de octubre de 2011.

VISTO:

La consulta realizada por OSE sobre la posibilidad de recolectar y tratar datos de salud del personal.

RESULTANDO:

Que por informe jurídico se recomienda a OSE la consideración de los principios legales en el tratamiento de datos especialmente protegidos. Asimismo por informe técnico se recomiendan una serie de medidas de seguridad a implementar.

CONSIDERANDO:

I) Que de acuerdo al artículo 9° de la Ley N° 18.331, no sería necesario el previo consentimiento informado, ya que se trata del ejercicio de una obligación legal. El mismo sí será necesario para ceder los datos fuera de OSE, a menos que se proceda a su disociación.

II) Que de acuerdo al Decreto N° 414/009, la base de datos creada debe ser inscripta ante la URCDP.

ATENTO:

A lo precedentemente expuesto y a lo dispuesto por la Ley N° 18.331.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales.

DICTAMINA:

I. RECOMENDAR A OSE TOMAR EN CONSIDERACIÓN LOS PRINCIPIOS DE LEGALIDAD, VERACIDAD, FINALIDAD, SEGURIDAD, RESERVA Y RESPONSABILIDAD DE LA LEY N° 18.331, ASÍ COMO LA IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD RESEÑADAS EN EL INFORME TÉCNICO.

II. RECOMENDAR A OSE TENER ESPECIALMENTE EN CUENTA LOS PRINCIPIOS DE FINALIDAD Y DE RESERVA EN LA COMUNICACIÓN INTERNA DE DATOS.

III. INDICAR A OSE LA INSCRIPCIÓN DE LA BASE DE DATOS CREADA, DE ACUERDO AL DECRETO N° 414/009.

IV. NOTIFÍQUESE Y PUBLÍQUESE.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
r.i.

Dictamen N° 24 de 28 de octubre de 2011.

Se dictamina sobre consulta del Servicio de Registro de Estado Civil de la Intendencia de Montevideo en relación con la publicación en la web de datos de las partidas.

DICTAMEN N°		EXPEDIENTE N°
24	2011	2011-2-10-000484

Montevideo, 28 de octubre de 2011.

VISTO:

La consulta recibida del Servicio de Registro de Estado Civil de la Intendencia de Montevideo, acerca de si la colocación en el sitio web institucional de la consultante, del índice archivo de las partidas de estado civil, se adecua al régimen jurídico de la protección de datos personales.

RESULTANDO:

I) Que se trataría de una publicación como "dato abierto", con acceso solamente al nombre completo de la persona; su fecha de nacimiento, matrimonio o defunción; año, sección y acta de inscripción.

II) Que en el sistema proyectado no se publicaría la imagen de la partida de estado civil asociada.

CONSIDERANDO:

I) Que el derecho a la protección de datos personales es un derecho inherente a la personalidad humana, reconocido como tal en el art. 72 de la Constitución de la República, y regulado por la Ley Nº 18.331, de 11-08-2008.

II) Que como tal, consagra una serie de principios básicos, derechos, obligaciones y garantías, para la protección del referido derecho.

III) Que la configuración de un sistema de publicidad como el propuesto, no obstante facilitar el acceso a quienes necesitan obtener esta tipo de documentos, se aparta del régimen legal, en la medida que un conjunto importante de datos que se proyectan publicar requerirían el consentimiento previo de sus titulares, extralimitando las excepciones previstas por los arts. 9º y 17 de la Ley.

ATENTO:

A lo expuesto, el informe jurídico precedente, y lo establecido por los arts. 72 de la Constitución de la República, 1º, 4º M), 5º, 9º y 17 de la Ley Nº 18.331, de 11 de agosto de 2008.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Que en el marco de la Ley Nº 18.331 de Protección de datos personales y Acción judicial de Habeas Data, la publicación con carácter abierto, en el sitio web de la Intendencia de Montevideo (Servicio de Registro de Estado Civil), de datos personales referidos a matrimonios, defunciones y cualquier otra especie, requiere de consentimiento previo de los afectados con las notas caracterizantes previstas en el art. 9º de la Ley.

2) Que quedan fuera de esta exigencia, los datos personales previstos en el art. 9º lit. C) de la misma Ley.

3) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

Dictamen N° 25 de 1 de noviembre de 2011.

Se dictamina sobre consulta realizada por la Dirección General de Comercio del Ministerio de Economía y Finanzas relativa al Acuerdo de Cooperación Técnica entre la República Federativa de Brasil y la República Oriental del Uruguay.

DICTAMEN N°		EXPEDIENTE N°
25	2011	2011-2-10-000752

Montevideo, 1 de noviembre de 2011.

VISTO:

La consulta recibida de la Dirección General de Comercio del Ministerio de Economía y Finanzas, poniendo a consideración de la Unidad, previo a su firma, el Acuerdo de Cooperación Técnica entre la República Federativa de Brasil y nuestro país.

RESULTANDO:

Que el referido Acuerdo contiene dos cláusulas vinculables al régimen competencial de la Unidad, y de modo general al derecho fundamental de la protección de datos personales.

CONSIDERANDO:

I) Que no rigen para el caso en consulta las excepciones al ámbito objetivo de la Ley Nº 18.331, de 11-08-2008, aplicándose ésta en toda su extensión no obstante la calidad de órganos públicos de las entidades que suscribirán el Acuerdo (artículo 3º de la Ley).

II) Que la Cláusula Primera del Acuerdo refiere a su "objeto", y no presenta dificultades de adecuación al régimen bajo contralor y tutela, en tanto y cuanto se entienda que su texto refiere exclusivamente a la transferencia unidireccional (de Brasil hacia Uruguay) de conocimientos técnicos y tecnología informática, conforme sentido natural y lógico que fluye de su lectura objetiva.

III) Que la Cláusula Cuarta refiere a "contrapartida" y "reciprocidad", y en este caso se alude a transferencias bidireccionales (de Brasil a Uruguay y viceversa), de informaciones provenientes de registros y actuaciones que contienen informaciones nominativas, donde las reparticiones especializadas de ambos países quedan recíprocamente autorizadas a divulgar y procesar tratamientos, de los registros provenientes del otro país, con la única salvaguarda de citar la fuente.

IV) Que en el caso de esta ulterior Cláusula, se asiste a una previsión que supone considerar como legítimas, de un modo general y anticipado, las transferencias internacionales de datos personales en la materia, entre ambos países, pero siendo Brasil un país que no cuenta con una declaración de nivel de protección adecuado en la materia, ello no resulta conforme al régimen cuyo control y tutela competen a esta Unidad.

V) Que la Unidad interviene preceptivamente en la autorización de las transferencias internacionales de datos personales, pudiendo admitirlas con arreglo al marco legal vigente y los elementos informativos que se le aporten, aún en casos como el presente donde se realizarían con un país que no dispone, a título general y declarado, de un nivel de protección adecuado a favor del derecho en juego.

VI) Que sin perjuicio del arbitrio de las partes para formular otro tipo de soluciones (como por ejemplo la eliminación de datos personales en los intercambios previstos), cabrá tener presente la sugerencia realizada por el Asesor Letrado preopinante en el expediente, proveyendo una redacción alternativa para la Cláusula Cuarta, que salvaría su cuestionamiento actual.

ATENTO:

A lo expuesto, el informe jurídico precedente, y lo establecido por los artículos. 72 de la Constitución de la República, 1º, 2º y 23 de la Ley Nº 18.331, de 11 de agosto de 2008; artículo 4º literales F) y H) y artículo 15 literal D) del Decreto Nº 414/009, de 31 de Agosto de 2009; Resolución Nº 17, de 12 de junio de 2009, Dictamen Nº 8, de 19 de marzo de 2010, e Informe Nº 76, de 29 de setiembre de 2009.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Que el Acuerdo de Cooperación Técnica a suscribirse el 4 de noviembre de 2011 entre las autoridades de la Defensa del Consumidor de la República Federativa de Brasil y nuestro país, es conforme al régimen de protección jurídica de los datos personales vigente en el país, salvo su Cláusula Cuarta – Contrapartida y Reciprocidad.

2) Que a los efectos de obtener una adecuación total del citado Acuerdo a las disposiciones nacionales vigentes, se deberán seguir los lineamientos previstos en los Considerandos del presente Dictamen, resultando igualmente útiles al efecto los aportes realizados en el Informe Nº 6922, de 27 de octubre de 2011.

3) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP

m.b.

Dictamen N° 26 de 4 de noviembre de 2011.

Se dictamina sobre la posibilidad que el Ministerio de Trabajo y Seguridad Social comunique los datos contenidos en las planillas de trabajo a la Dirección Nacional de Bomberos a efectos de contralor que las empresas cuenten con habilitación de bomberos.

DICTAMEN N°		EXPEDIENTE N°
26	2011	2011-2-10-0000646

Montevideo, 4 de noviembre de 2011.

VISTO:

La consulta presentada por la Dirección Nacional de Bomberos.

RESULTANDO:

I. Que la consulta refiere a la posibilidad de que el Ministerio de Trabajo y Seguridad Social comunique datos contenidos en las planillas de trabajo llevadas por aquél, a la Dirección Nacional de Bomberos con el objetivo de controlar que las empresas que cuentan con habilitación de Bomberos mantengan personal capacitado en el marco de los cursos de capacitación externa que brinda dicha Institución.

II. Que el expediente pasó a informe jurídico, el cual se realizó con fecha 12 de octubre de 2011.

CONSIDERANDO:

I. Que estamos ante la presencia de datos personales contenidos en las planillas de trabajo llevadas por el Ministerio de Trabajo y Seguridad Social, por lo que es aplicable al caso concreto la Ley Nº 18.331, de 11 de agosto de 2008 de Protección de Datos Personales.

II. Que la consulta presentada refiere a una comunicación de datos entre el Ministerio de Trabajo y Seguridad Social y la Dirección Nacional de Bomberos.

III. Que según el artículo 17º de la Ley, los datos personales objeto de tratamiento 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.

IV. Que el artículo mencionado establece además los casos, en forma taxativa, en que no será necesario el consentimiento del titular de los datos para su comunicación. Entre las hipótesis previstas se encuentran los supuestos determinados por el artículo 9º de la Ley.

V. Que en el caso consultado sería aplicable la excepción relativa a que no es necesario el consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, la cual es aplicable por la remisión que hace el literal B) del artículo 17º de la Ley.

VI. Que la Dirección Nacional de Bomberos solicita al Ministerio de Trabajo las planillas de trabajo

presentadas por las empresas con el objetivo de controlar que éstas cumplan con la obligación legal que establece la Ley Nº 15.896. Por lo tanto, solicita los datos en virtud del cumplimiento de cometidos específicos que le son asignados por la Ley.

VII. Que en la presente consulta se verifica la excepción contenida en el artículo 9° literal B) de la Ley, por lo que la comunicación de datos es legítima ya que la Dirección Nacional de Bomberos está ejerciendo funciones propias del organismo y los datos provienen de otro organismo, por lo que no sería necesario recabar el consentimiento de los titulares.

VIII. Que igualmente se hace aplicable el resto de la normativa vigente, sobre todos los principios que regulan la protección de datos.

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:

I - Establecer que es legítima la comunicación de datos entre el Ministerio de Trabajo y Seguridad Social y la Dirección General de Bomberos.

II - Indicar que no es necesario recabar el consentimiento de los titulares porque se verifica la excepción relativa al ejercicio de las funciones propias de los organismos.

III - Recomendar que se tengan presentes las demás disposiciones relativas a la protección de datos.

IV - Notifíquese, y oportunamente publíquese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
j.h.

Dictamen N° 27 de 4 de noviembre de 2011.

Se dictamina sobre la posibilidad que el Hospital de Clínicas comunique datos de los pacientes que reciben tratamiento por consumo de tabaco al Fondo Nacional de Recursos para que se les brinde la medicación necesaria.

DICTAMEN N°		EXPEDIENTE N°
27	2011	2011-2-10-0000678

Montevideo, 4 de noviembre de 2011.

VISTO:

La consulta realizada por el Hospital de Clínicas a la Universidad de la República.

RESULTANDO:

I. Que la consulta refiere a la posibilidad de que el Hospital de Clínicas comunique datos de los pacientes que reciben tratamiento por tabaco, al Fondo Nacional de Recursos, a efectos de que éste último brinde la medicación necesaria. Para ello recaba el consentimiento de los titulares de los pacientes y consigna la información en un formulario diseñado a esos efectos.

II. Que también se consulta sobre la creación de una base de datos por parte del Fondo Nacional de Recursos cuya información será utilizada para confeccionar estadísticas en forma disociada.

III. Que el expediente pasó a informe jurídico, realizándose éste con fecha 19 de octubre del presente año.

CONSIDERANDO:

I. Que la consulta trata sobre datos personales conforme con la definición contenida en el artículo 4° literal d) de la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP).

II. Que la consulta refiere a una comunicación de datos del Hospital de Clínicas al Fondo Nacional de Recursos respecto de los pacientes a los cuales se prescribe medicación para curar el tabaquismo.

III. Que la LPDP indica que comunicación de datos es toda revelación de datos realizada a una persona distinta del titular de los datos. En este sentido, la LPDP indica que la comunicación de datos debe ser realizada con el consentimiento de las partes y en relación con el interés legítimo del emisor y del destinatario, así como informar sobre la finalidad de la comunicación e identificar al destinatario.

IV. Que en la consulta se verifican todos los requisitos exigidos por la norma, en tanto se considera que el Hospital de Clínicas como el Fondo Nacional de Recursos están actuando dentro de las funciones a ellos asignadas.

V. Que en lo que tiene relación con el consentimiento del titular, se considera adecuado el medio instrumentado y los datos requeridos. Y que, en relación con el alcance del consentimiento, se entiende que se debe informar tanto respecto a la recolección como del tratamiento de los datos personales.

VI. Que respecto a la posibilidad de aplicar algunas de las excepciones del artículo 17 a la LPDP se debe considerar que la Ley N° 17.793, de 16 de julio de 2004, hace aplicable en el país el Convenio Marco de la Organización Mundial de la Salud por el cual se deben establecer centros de salud y de rehabilitación así como programas de diagnóstico, asesoramiento, prevención y tratamiento del tabaco

VII. Que en el caso de marras se trata de organismos públicos actuando dentro de sus competencias y en cumplimiento de la Ley N° 17.793, de 16 de julio de 2004, por lo que sería aplicable al caso concreto el literal c) del artículo 17 de la LPDP.

VIII. Que se considera correcto y necesario el acceso por parte de personal autorizado del Fondo Nacional de Recursos a la base de datos creada a esos efectos siempre que se cumpla con el principio de seguridad de los datos.

IX. Que es correcto que el Fondo Nacional de Recursos realice estadísticas disociándose los datos personales sometidos a tratamiento conforme la normativa vigente.

X. Que se deben respetar todos los principios que regulan la protección de datos, sobre todo lo relativo a los principios de seguridad y veracidad de los datos.

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:

I - Expedirse en el sentido consignado en los Considerandos IV a X del presente dictamen.

II - Notifíquese, y oportunamente publíquese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
f.b.

Dictamen N° 28 de 4 de noviembre de 2011.

Se dictamina sobre la posibilidad que el Ministerio de Trabajo y Seguridad Social comunique datos contenidos en las planillas de trabajo al Ministerio de Transporte y Obras Públicas.

DICTAMEN N°		EXPEDIENTE N°
28	2011	2011-2-10-0000687

Montevideo, 4 de noviembre de 2011.

VISTO:

La consulta presentada por el Ministerio de Transporte y Obras Públicas.

RESULTANDO:

I. Que la consulta refiere a la posibilidad de que el Ministerio de Trabajo y Seguridad Social comunique datos contenidos en las planillas de trabajo llevadas por aquél, al Ministerio de Transporte y Obras Públicas. La finalidad de la mencionada solicitud radica en el diseño por parte del MTOP de un Sistema de Información de Transporte de Carga Terrestre y guías de carga. Para el ingreso en las guías es necesario verificar que los profesionales registrados o que estén enviando información pertenezcan a la empresa correspondiente.

II. Que el expediente pasó a informe jurídico, el cual se realizó con fecha 18 de octubre de 2011.

CONSIDERANDO:

I. Que estamos ante la presencia de datos personales contenidos en las planillas de trabajo llevadas por el Ministerio de Trabajo y Seguridad Social, por lo que es aplicable al caso concreto la Ley Nº 18.331, de 11 de agosto de 2008 de Protección de Datos Personales.

II. Que la consulta presentada refiere a una comunicación de datos entre el Ministerio de Trabajo y Seguridad Social y el Ministerio de Transporte y Obras Públicas.

III. Que según el artículo 17º de la Ley, los datos personales objeto de tratamiento 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.

IV. Que el artículo mencionado establece además los casos, en forma taxativa, en que no será necesario el consentimiento del titular de los datos para su comunicación. Entre las hipótesis previstas se encuentran los supuestos determinados por el artículo 9º de la Ley.

V. Que en el caso consultado sería aplicable la excepción relativa a que no es necesario el consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, la cual es aplicable por la remisión que hace el literal B) del artículo 17º de la Ley.

VI. Que el Ministerio de Transporte y Obras Públicas solicita los datos en virtud del cumplimiento de cometidos

específicos que le son asignados por la Ley. En el caso, solicita al Ministerio de Trabajo y Seguridad Social las planillas de trabajo presentadas por las empresas con el objetivo de gestionar el sistema antes mencionado. Por ello, podríamos concluir que dichos datos se recaban en el marco del ejercicio de sus funciones propias.

VII. Que en la presente consulta se verifica la excepción contenida en el artículo 9° literal B) de la Ley, por lo que la comunicación de datos es legítima ya que el Ministerio de Transporte y Obras Públicas está ejerciendo funciones propias del organismo y los datos provienen de otro organismo, por lo que no sería necesario recabar el consentimiento de los titulares.

VIII. Que correspondería tener en cuenta también la excepción dispuesta en el artículo 9º literal C) de la Ley. En él se indican los datos correspondientes a personas físicas que no requieren el previo consentimiento del titular para su tratamiento: nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. De acuerdo con lo informado en la consulta se comunicarán únicamente los nombres y apellidos y el documento de identidad de los empleados. En este caso, y de acuerdo a la excepción analizada, se trataría de datos que no requerirían de previo consentimiento del titular para su comunicación.

IX. Que igualmente se hace aplicable el resto de la normativa vigente, sobre todo los principios que regulan la protección de datos.

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:

I - Establecer que es legítima la comunicación de datos entre el Ministerio de Trabajo y Seguridad Social y el Ministerio de Transporte y Obras Públicas.

II - Indicar que no es necesario recabar el consentimiento de los titulares porque se verifican las excepciones dispuestas en el artículo 9º literales B) y C) de la Ley.

III - Recomendar que se tengan presentes las demás disposiciones relativas a la protección de datos.

IV - Notifíquese, y oportunamente publíquese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
j.h.

Dictamen N° 29 de 18 de noviembre de 2011.

Se dictamina sobre la legalidad de comunicar datos personales a un gremio de una entidad pública.

DICTAMEN N°		EXPEDIENTE N°
29	2011	2011-2-10-0000542

Montevideo, 18 de noviembre de 2011.

VISTO:

La consulta que formula el Sr. Wilson Flores, en relación a la legalidad de la comunicación de sus datos personales al gremio de ANTEL, por parte de esta empresa estatal.

RESULTANDO:

I) Que la consulta refiere a Nombre y apellido, Domicilio, Documento de identidad, Fecha de nacimiento, Nacionalidad, Número de teléfono e interno institucionales, Correo electrónico institucional y Clase de trabajo.

II) Que se parte del supuesto de que el consultante reviste como funcionario de la empresa estatal mencionada.

CONSIDERANDO:

I) Que los datos personales que motivan la consulta constituyen "información pública", y por lo tanto son pasibles de difusión a terceros.

II) Que con arreglo a la anterior premisa, el consultante no puede oponerse a su comunicación en los términos indicados en la consulta.

III) Que, en cambio, dispone del "derecho de supresión" que le confiere la ley de la materia sobre los datos comunicados, el que podrá ejercitar exclusivamente sobre aquellos tratamientos y bases de datos que lleve a cabo el gremio a partir de la referida comunicación.

ATENTO:

Al Informe jurídico emitido, a lo expuesto y lo establecido en los arts. 2º, y 5º de la Ley N° 18.381, de 17 de Octubre de 2008, 15 y 21 de la Ley Nº 18.331, de 11 de Agosto de 2008.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1.- Que el funcionario de una entidad estatal no puede oponerse a que el órgano del cual depende comunique a terceros su Nombre y apellido, Domicilio, Documento de identidad, Fecha de nacimiento, Nacionalidad, Número de teléfono e interno institucionales, Correo electrónico institucional y Clase de trabajo, ya que se

trata de información pública.

2.- Que sin perjuicio de ello, el titular de los datos puede ejercer el derecho de supresión de todos o algunos de los datos comunicados, exclusivamente en lo que refiere a los nuevos tratamientos y bases de datos que realice o disponga el receptor, cuando -como en el caso de un gremio- no existe un interés superior que prevalezca a fin de mantenerlos aún sin su consentimiento.

3.- Notifíquese, publíquese, etc.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

Dictamen N° 30 de 18 de noviembre de 2011.

Se dictamina sobre la consulta recibida por la Administración Nacional de Educación Pública (ANEP) relativa al régimen que se sigue en un centro educativo para la publicidad en las carteleras de las inasistencias de los funcionarios.

DICTAMEN N°		EXPEDIENTE N°
30	2011	2011-2-10-0000562

Montevideo, 18 de noviembre de 2011.

VISTO:

La consulta recibida de la abogada contratada de ANEP con residencia en Río Negro, Dra. Ximena Centurión Maza, poniendo a consideración de la Unidad, el régimen que se sigue en su centro educativo en materia de publicidad de inasistencias de funcionarios.

RESULTANDO:

I) Que de acuerdo a lo manifestado por la consultante, la Institución posee una cartelera con fines informativos.

II) Que una parte de esta cartelera, bajo el título INASISTENCIAS, publicita las ausencias de los funcionarios, si la misma fue con o sin aviso, y en el segundo caso el artículo del Estatuto del Funcionario que la ampara, entre otros datos.

III) Que la consultante desea saber si este tipo de publicaciones entra en conflicto con las disposiciones de la Ley Nº 18.331, y en su caso las acciones que eventualmente podrían iniciarse de ser vulnerados los derechos protegidos por la mencionada Ley.

CONSIDERANDO:

I) Que de principio, la publicidad de este tipo de hechos en carteleras ubicadas en el interior de los recintos de enseñanza pública, resulta un instrumento legal e idóneo, no requiriendo el consentimiento previo de los titulares de los datos para su puesta en práctica.

II) Que el fundamento de tal legalidad radica en el hecho de que se trata de un medio de control jerárquico y social, esto último en instancia razonablemente acotada al ámbito donde el funcionario cumple labores, al servicio del cumplimiento efectivo de uno de los principales deberes del cargo.

III) Que la reglamentación vigente no impide este tipo de publicidad no obstante lo cual, y a la luz de los modernos principios en la materia, se deben observar en su ejercicio los principios de veracidad, finalidad y proporcionalidad, prescriptos por la Ley Nº 18.331.

IV) Que sin perjuicio de la licitud de esta práctica en los términos establecidos, la consultante, y titulares

afectados en general, disponen de las facultades que les otorga la misma Ley, a los efectos de exigir rectificaciones, actualizaciones, inclusiones y supresiones de sus datos cuando ello corresponda, pudiendo asimismo ejercitar la acción judicial de habeas data cuando el responsable de la publicación desoyera sus legítimos reclamos practicados en la vía administrativa.

ATENTO:

A lo expuesto, el informe jurídico precedente, y lo establecido por los artículos 7º, 8º, 9º inciso tercero literal B), 15, 37 y siguientes de la Ley Nº 18.331, de 11 de agosto de 2008,
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1) Que la publicación de las inasistencias de funcionarios docentes y no docentes en centros de enseñanza, resulta conforme a la Ley Nº 18.331, y no requiere el consentimiento previo de los titulares de los datos para llevarse a cabo.

2) Que a los efectos de asegurar esta conformidad, la publicación debe ser efectuada con arreglo a los principios y previsiones que emanan del régimen en la materia, entre otros que se publiquen datos veraces, ecuánimes y no excesivos, debiendo ser eliminados cuando se entienda cumplida la finalidad de este tipo de difusión.

3) Que sin perjuicio de la legalidad de esta práctica, los titulares de los datos personales publicados disponen de las facultades de autodeterminación informativa para controlar la calidad de sus datos publicados, pudiendo ejercer el derecho de rectificación, actualización, inclusión o supresión, así como la acción judicial de habeas data cuando el responsable de la publicación desoyera un reclamo del tenor anotado, y legítimo a juicio del afectado.

4) Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

Dictamen N° 31 de 7 de diciembre de 2011.

Se dictamina sobre la aprobación del proyecto de reglamentación del Sistema de Información Integrada del Área Social (SIIAS) aportado por el Ministerio de Desarrollo Social.

DICTAMEN N°		EXPEDIENTE N°
31	2011	2011-2-10-0000950

Montevideo, 7 de diciembre de 2011.

VISTO:

El proyecto de reglamentación del SIIAS (Sistema de Información Integrada del Área Social) aportado por el Ministerio de Desarrollo Social, sometido a dictamen de la Unidad en cumplimiento del art. 621 inc. 2º de la Ley Nº 18.719.

RESULTANDO:

I) Que los textos sometidos a dictamen constan de un Anteproyecto de Decreto Ministerial y un Modelo de Convenio a ser suscripto por las entidades partícipes del Sistema.

II) Que asimismo se han producido instancias de diálogo entre el personal técnico afectado a las máximas instancias de este Sistema, y los Asesores de la Unidad, las que han permitido ilustrar los alcances de aquél y su inserción en el régimen de la Ley Nº 18.331.

CONSIDERANDO:

I) Que se trata de un sistema integrador de informaciones relativas a prestaciones sociales, provenientes y al servicio de la operativa de diversas instituciones públicas.

II) Que, como lo expresa el propio Anteproyecto de Decreto Ministerial, los datos que se almacenarán en el referido Sistema, serán recabados y utilizados en ejercicio de funciones propias de los poderes del Estado y de conformidad con mandatos legales.

III) Que los textos propuestos atienden a especificidades del Sistema con relación al régimen general de la Ley Nº 18.331, mereciendo dictamen favorable por ajustarse, en lo racionalmente atendible, a los principios y obligaciones de la Ley.

ATENTO:

Al Informe jurídico emitido, a lo expuesto, y a lo establecido en los arts. 9º lit. B) del inc. 3º, 17 lit. A) del inc. 3º y 18 inc. 2º de la Ley N° 18.331, de 11 de Agosto de 2008; y en los arts. 159 y 621 inc. 2º de la Ley Nº 18.719, de 27 de Diciembre de 2010.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1.- Aprobar el Proyecto de reglamentación del SIIAS (Sistema de Información Integrada del Área Social) aportado por el Ministerio de Desarrollo Social y cuyos textos se incorporan al presente Dictamen por vía de Anexos.

2.- Notifíquese, publíquese, etc.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

Dictamen N° 32 de 27 de diciembre de 2011.

Se dictamina en relación con la necesidad que el titular de una cédula de identidad preste su consentimiento para entender que es conforme a derecho la generación del servicio de control de identidad de la Dirección Nacional de Identificación Civil.

DICTAMEN N°		EXPEDIENTE N°
32	2011	2011-2-10-0000725

Montevideo, 27 de diciembre de 2011.

VISTO:

La consulta formulada en relación a si es necesario que el titular de una cédula de identidad preste su consentimiento para entender conforme a derecho la generación del servicio de la DNIC (Dirección Nacional de Identificación Civil) de control de identidad que retorna la información contenida en ambos lados del citado documento.

RESULTANDO:

I) Que dicho servicio supone una consulta en línea por parte de quien debe realizar el control de identidad, confrontando los datos del documento recibido con los existentes en la citada Dirección.

II) Que para ello se requiere ingresar el "número de hoja interior", y por tanto, quien realiza la consulta, ha de tener en su poder la cédula de la persona sujeta a identificación, retornando datos incluidos en el documento incluyendo el sexo del involucrado.

CONSIDERANDO:

I) Que cuando una persona presenta en un trámite la cédula de identidad, se entiende que está dando su consentimiento para que se acceda a los datos que figuran en el documento, acorde a una finalidad determinada por el trámite que se desea realizar, y para el cual es necesario identificarse.

II) Que la visualización en pantalla del referido documento en versión electrónica, no resulta violatoria de la Ley Nº 18.331 y, por el contrario, configura una garantía ciudadana, en cuanto a verificar la fidelidad del documento utilizado y coartar el uso de documentos falsos o cambiados.

III) Que lo expresado no equivale a permitir tratamientos diversos al expresado, quedando absolutamente inhibida la creación de nuevas bases de datos a partir de la información consignada, a modo de ejemplo almacenar fotografías, firmas o huellas digitales, todo lo cual requeriría el previo consentimiento informado de los titulares de los datos, para cualquier otro tipo de tratamiento diferente al expresado, incluyendo la comunicación o cesión de datos.

ATENTO:

A los informes consignados, a lo expuesto, y lo establecido en los arts. 8º y 9º de la Ley N° 18.331, de 11 de Agosto de 2008.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1.- Que el servicio de identificación de personas en línea que provee la DNIC (Dirección Nacional de Identidad), por el que simplemente se permite visualizar electrónicamente la información contenida en la cédula de identidad de la persona, para validarla, resulta conforme a los principios y deberes de la Ley Nº 18.331, de 11 de agosto de 2008.

2.- Notifíquese, publíquese, etc.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo
URCDP
m.b.

Informe N° 137 de 11 de enero de 2011.

Se informa consulta relativa a la posibilidad de crear una base de datos similar a una guía telefónica.

INFORME N°		EXPEDIENTE N°	
137	2011	001	2011

Montevideo, 11 de enero de 2011.
Ref. Consulta sobre la creación de base de datos personales.

- I -ANTECEDENTES

Con fecha 10 de octubre de 2010, el Sr. Hugo Álvarez se presentó ante la Unidad Reguladora y de Servicios de Comunicaciones (URSEC) a efectos de formular consulta acerca de la creación de una base de datos de la cual cualquier persona puede formar parte, conjugándose de esta forma en una especie de guía telefónica.

Por nota de fs. 22 del expediente principal (N° 2010/1/01056), la URSEC resolvió remitir las actuaciones a la Unidad Reguladora y de Control de Datos Personales (URCDP), en el entendido que ésta posee las competencias legales pertinentes para el análisis de los presentes obrados.
Con fecha 3 de enero del presente año se recibieron dichas actuaciones, y el 4 del mismo mes el expediente pasó a informe jurídico.

-II- INTRODUCCION

En síntesis la consulta versa sobre los siguientes puntos:
- Creación de una base de datos que contendrá datos de los teléfonos celulares de los titulares, el nombre, domicilio, entre otra información.
- Se realizará siempre con consentimiento del titular, el que en cualquier momento podrá solicitar la eliminación de la información proporcionada.
- Se brindan una serie de ejemplos de donde surge que las finalidades de la base de datos serían de contacto y ubicación de personas.

-III-ANALISIS

-Concepto de base de datos y deberes del Responsable-
El artículo 4° literal A) de la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas data (en adelante Ley N° 18.331), define a las bases de datos como un 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.

Por otra parte, dicha ley prevé una serie de obligaciones que el responsable de la base de datos o del tratamiento debe cumplir.

Según surge de fs. 18, estamos en presencia de una base de datos personales, que incluye los datos del nombre, domicilio, y teléfono celular de los titulares, donde el consultante aparece como responsable de ésta.
En cuanto a las obligaciones del consultante como responsable de la base de datos y sin intención de realizar una descripción detallada de las mismas, se destacan a continuación algunas de ellas.

a) deber de inscripción de la base de datos: el responsable de la base de datos deberá registrar la base de datos a crear en un plazo de 90 días a partir del inicio de las actividades -art. 17 Decreto N° 414/009, de 31 de agosto de 2009-.
Se considera que, de una interpretación armónica de este artículo con el resto de la normativa, la inscripción de la base de datos se debe realizar una vez iniciadas las actividades con dicha base de datos, más precisamente, una vez comenzado a realizarse el tratamiento sobre la información.
El requisito de inscripción, es indispensable para que la base de datos sea legal y se adecue a los parámetros establecidos en la normativa vigente de protección de datos personales.

b) Conforme a la consulta formulada, resulta fundamental que el responsable prevea mecanismos por los cuales se asegure:
- la disponibilidad de la información, es decir que los datos se organicen y almacenen de una forma adecuada que permita el ejercicio de los derechos de los titulares de los datos -inc. 2° art. 10 Ley N° 18.331-;
- la confidencialidad de la información, por la cual todo aquel que por su situación laboral u otra forma de relacionamiento con el responsable acceda o intervenga en cualquier etapa del tratamiento de datos personales deberán ser manejados de forma reservada;
- la integridad de la información, por la cual los datos deberán permanecer inalterados, por lo que toda modificación de dicha información deberá ser autorizada.

c) cumplimiento de los principios en la materia: en sede de protección de datos personales existen una serie de principios generales que sirven de criterios orientadores a efectos de la interpretación y aplicación de las normas en la materia.
En tal sentido, resulta determinante que el consultante respete en especial, el principio de finalidad y el principio del previo consentimiento.
Para ello, deberá informar de manera previa y expresa a todo titular -interesado en acceder a la base de datos objeto de consulta-, la identidad y domicilio del responsable, la posibilidad de ejercer los derechos previstos en la normativa, y fundamentalmente la finalidad para la cual los datos serán tratados y quiénes pueden ser los destinatarios de la información en caso que los datos sean comunicados.
Se desprendería que la finalidad de contacto y ubicación de personas, determina que los datos sean constantemente comunicados a otras personas. Por tanto, el titular deberá ser informado de dicho extremo con anterioridad a ser incluido en la base de datos, debiendo decidir si permite dicha circunstancia.
Asimismo, se destaca que es importante que los titulares conozcan detalladamente la finalidad para la cual los datos van a ser tratados y comunicados, pudiendo optar por no integrar la base, o integrarla

solamente para una finalidad en específico. Si la finalidad de la comunicación se modifica, se deberá solicitar nuevamente el consentimiento de éste para que dicha comunicación se realice de acuerdo con la ley.

d) se deberá informar a los titulares que disponen de los derechos de acceso, rectificación y supresión de sus datos personales, pudiéndolos ejercer en cualquier momento y sin necesidad del abono de contraprestación alguna. Con carácter general, podemos decir que, el derecho de acceso es el derecho por el cual el titular puede conocer toda la información que de su persona se encuentre en la base de datos. El derecho de rectificación, es aquél donde el titular puede modificar la información proporcionada o almacenada en una base de datos por resultar ésta inexacta o incompleta. Y por su parte, en el derecho de supresión el titular tiene derecho a solicitar la eliminación de su información personal, cuando ésta sea inadecuada, excesiva, o su utilización por terceros resulte ilegítima.

Cabe agregar que la normativa de protección de datos también prevé otros derechos, tales como el de inclusión, actualización y bloqueo de datos.
Todos estos derechos se deben ejercer bajo los parámetros legales y reglamentarios establecidos, donde el responsable deberá conceder el acceso, rectificación o proceder a la eliminación de la información en el plazo de cinco días hábiles a partir de recibida la solicitud. El incumplimiento de dicha obligación, habilita al titular a iniciar la acción judicial de habeas data ante los tribunales.
Por otra parte, cabe destacar que el consultante adjunta modelos de formularios para ingresar a la base de datos objeto de consulta, los que lucen a fs. 4, 5 del expediente principal.
En cuanto al documento de fs. 4 referido, se considera que no resultaría adecuada la leyenda “acepto las condiciones impuestas por GUICELCO y o URSEC a efectos de ampliar la utilización de mi celular y/o autorizado por URSEC”.

A la luz de la normativa de protección de datos personales, es el titular quien tiene el derecho de conocer, disponer y controlar la información que le concierne. Por lo que, en primer lugar, es quien debe ser informado siempre de manera previa al ingresar a una base de datos acerca de las condiciones a las que refiere el consultante. Estas condiciones deben ser claras, concretas y estar disponibles para el titular.
En segundo lugar, los métodos de tratamiento, procesamiento y almacenamiento de la información, los define el responsable de la base de datos, por tanto, no es URSEC y tampoco la URCDP, quienes realizan esta tarea. La URCDP como órgano competente en materia de protección de datos, tiene la potestad legal de realizar todas las tareas necesarias para garantizar el efectivo cumplimiento de los objetivos y disposiciones de la normativa. Conforme a ello, es ésta quién controlará si el responsable adecua sus actividades a la normativa.

En consecuencia, se sugiere la readecuación del formulario presentado a fs. 4 “Certificado de Afiliación”. Para ello, se recomienda acceder al sitio web de la URCDP -www.datospersonales.gub.uy, y descargar los formularios de: Cláusula de Consentimiento informado, formulario para el ejercicio de los derechos de acceso, rectificación, inclusión y supresión.

En definitiva, se sugiere al consultante la adopción de los formularios disponibles en el sitio web señalado, dejando sin efecto el presentado a fs. 4, por no corresponderse adecuadamente con la normativa en la materia.
En referencia al formulario de fs. 5, se recomienda la modificación de la leyenda"dejo constancia de no divulgar este número sin previo consentimiento de esta Base y/o titular de acuerdo a reglas de URSEC".

La referencia a URSEC no resulta adecuada de acuerdo con lo mencionado precedentemente. Además, tal como hemos hecho referencia, el consentimiento es otorgado por el titular y no por la base de datos. En este sentido, dicho consentimiento deberá ser recabado de forma expresa dejando prueba del mismo, debiendo también dejarse constancia de la revocación de dicho consentimiento.

Por lo tanto, y a efectos de un mejor análisis, se sugiere se solicite al consultante la presentación de este formulario tomando en cuenta las recomendaciones realizadas. Dicha presentación, podrá realizarse de manera conjunta con el formulario de base de datos.
-Tipos de datos tratados y soporte de almacenamiento-
En cuanto a los datos tratados, no se informa por parte del consultante la totalidad de información que se alojará en la base de datos, debido a que sólo se proporciona información acerca del tratamiento de datos identificatorios. En principio, se trataría de datos personales pertenecientes a personas físicas, en virtud que dicho extremo no resulta aclarado.

De acuerdo con lo establecido en literal c) del artículo 9° de la Ley N° 18.331, se debe tener presente que si bien el nombre y domicilio de los titulares no necesitan del previo consentimiento informado, sí el teléfono celular de las personas físicas.
En efecto, dentro de los extremos no informados por el consultante, no surge el mecanismo y fuente o fuentes de recolección de la información. Punto que es de vital importancia. Por tanto, se considera que se deberá tener presente que la recolección de datos personales deberá realizarse de acuerdo con los parámetros dispuestos en la normativa.
En referencia al soporte de almacenamiento de los datos, no resultan claras las manifestaciones del Sr. Álvarez. En efecto, se desprendería de la consulta planteada, que se trataría de un soporte informático. Asimismo, el consultante se refiere a una "base móvil" -punto 5 fs. 19-, por lo que en este caso, una de las posibilidades sería que se tratare de un sitio web donde se registren los titulares.

-IV- CONCLUSIONES

Del análisis de la consulta planteada, se verifica que la creación de una base de datos personales con las finalidades descriptas no contradice, en principio y en teoría, la normativa de protección de datos personales.
Sin embargo, y a los efectos de un mejor análisis de los extremos expuestos en el presente informe, -fundamentalmente en cuanto a los deberes por parte del consultante como responsable de la base de datos-, se recomienda se solicite al Sr. Álvarez la realización del procedimiento de inscripción de la base de

datos de forma inmediata, una vez iniciadas las actividades pretendidas. Dicha recomendación, es atento al principio de legalidad previsto en el artículo 6° de la Ley N° 18.331.

Para el cumplimiento del proceso de inscripción referido, se deberá ingresar al sitio web de la Unidad, www.datospersonales.gub.uy, completar el formulario a estos efectos, y realizar la presentación papel del formulario señalado.

Asimismo, se realizaron recomendaciones en cuanto a los formularios adjuntados por el consultante, en donde se sugirió la presentación del que luce a fs. 5 a efectos de su análisis de adecuación con los parámetros y criterios legales y reglamentarios. Dicha presentación, podrá efectuarse conjuntamente con el formulario de base de datos, tal como se señaló anteriormente.

Fdo. Dr. Federico Carnikian
Derechos Ciudadanos

Informe N° 1023 de 31 de enero de 2011.

Se informa denuncia relativa a la utilización del número telefónico del denunciante.

INFORME N°		EXPEDIENTE N°	
1023	2011	3417	2010

Montevideo, 31 de enero de 2011.
Ref. Denuncia José Luis Regueiro c/ UTE.

Con fecha 18 de noviembre de 2010 se presenta denuncia ante la Unidad, por utilización, por parte de UTE, del número telefónico del denunciante. El hecho habría ocurrido en oportunidad de que esta persona tramitara un pedido de acceso a información conforme Ley Nº 18.381. La queja se sustenta en que el citado número telefónico no figuraba en la petición y, si bien consta en la guía telefónica, no lo está a su nombre (fs. 2). Vista mediante, la denunciada comparece aportando copia auténtica de la información proporcionada al denunciante a través de correo electrónico, y afirmando que "no surge de la misma [nota: refiere a la copia del expediente respectivo] que se hayan realizado comunicaciones telefónicas de ninguna especie entre UTE y el denunciante" (fs. 26). La afirmación de la denunciada dejó margen a la duda puesto que el denunciante pone su planteo a consideración de la URCDP el 18 de noviembre (fs. 2), mientras que el Ente requerido termina proporcionando la información recién el 29 de noviembre (fs. 22 y 23).

Por tal motivo se solicitó mayor ilustración de cargo de la denunciada (fs. 27), la que fue satisfecha a fs. 38 aportándose testimonio auténtico del contrato de suministro de energía eléctrica otorgado entre las partes (fs. 36-37). Estando ahora completa la instrucción, se concluye que no existe mérito para sancionar a la denunciada y así se aconsejará. En el caso, el ejercicio del derecho de acceso de información a través de la petición formulada por el denunciante ante la denunciada, con arreglo a la Ley Nº 18.331, tiene relación en última instancia con el "contrato de suministro de energía eléctrica" agregado a fs. 36-37.
Es claro que el denunciante proporcionó su número telefónico al contratar el servicio, lo cual equivale a prestar consentimiento para un uso normal y mínimo del mismo, o sea para comunicaciones entre las partes del contrato (arts. 1261 y ss. del Código Civil, art. 9º inc. 3º lit. D) de la Ley Nº 18.331).

No consta en autos que la denunciada haya empleado realmente el número telefónico para comunicarse con el denunciante. Es la versión que aporta el denunciante. Pero aunque lo hubiere hecho, no aparecen probadas ningún tipo de conductas irregulares, ya sea con dicho uso o a partir del mismo. Por lo demás, se equivoca el denunciante cuando sostiene que "la comunicación frente a un pedido de información debe hacerse únicamente por las vías indicadas en la petición...", en tanto el art. 13 lit. C) de la Ley Nº 18.381 expresa lo contrario.

Sin perjuicio de todo lo expresado, se sugerirá dirigir una recomendación a la denunciada que suponga tomar previsiones tendientes a evitar nuevos episodios como el ocurrido.

Previo a dictarse resolución, se dará vista de lo actuado a denunciante y denunciado (arts. 75 y 76 del Decreto Nº 500/991).

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 1629 de 8 de febrero de 2011.

Se informa consulta en relación con la pertinencia de inscripción de las bases de datos del Sistema Informático de Compras Estatales.

INFORME N°		EXPEDIENTE N°	
1629	2011	19	2011

Montevideo, 8 de febrero de 2011.
Ref. Consulta inscripción base de datos SICE.

Se consulta si corresponde registrar como base de datos la información de los usuarios que utilizan el SICE (Sistema de Información de Compras Estatales) y la página www.compraestatales.gub.uy

Se expresa que los usuarios son funcionarios de la Administración Pública que publican los procedimientos de compras de acuerdo a requisitos y procedimientos estatuidos por los Decretos 342/999 cap. 2 y 289/002. Y que para ello se requiere de cada usuario un conjunto de datos personales, a saber: inciso, unidad ejecutora, unidad de compra, nombre y apellido, número de cédula de identidad, teléfono de la oficina donde cumple función, dirección de correo institucional, dirección de correo particular cuando lo ha enviado para recibir la contraseña por no tener el institucional, y la referida contraseña personal.

A requerimiento previo a informar (fs. 2), se aclara que el conjunto de los datos enunciados reúne la calidad de base de datos, de conformidad con la definición legal que proporciona el art. 4º núm. 1º de la Ley Nº 18.331.
La consultante amplía y plantea su duda en cuanto a "si corresponde registrar esa base... porque son los datos mínimos necesarios para ingresar a trabajar el sistema... datos mínimos para ingresar a trabajar al sistema... es como una parte imprescindible del sistema... similar a los datos que tiene por ejemplo AGESIC de cada uno de los que tenemos acceso a la red interna".

Entendemos que la base de datos objeto de consulta ingresa en el ámbito objetivo de aplicación de la Ley Nº 18.331, salvo lo referente a la exigencia del consentimiento de los titulares afectados, terreno este último en el que juega la excepción del art. 9º inc. 3 lit. B) de la misma Ley: "...ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".
En efecto, las únicas bases de datos excluidas del ámbito objetivo de la Ley son las consignadas en su art. 3º la que motiva la consulta, no ingresa en ninguna de las categorías indicadas en dicha norma legal. Por ende, estamos ante una base de datos cuyo registro es obligatorio, de conformidad con el art. 29 de la misma Ley.

Se concluye e informa:
Que la base de datos de funcionarios públicos usuarios del Sistema SICE debe registrarse ante la URCDP, de conformidad con el art. 29 de la Ley Nº 18.331.

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 4101 de 10 de marzo de 2011.

Se informa denuncia relativa a no haber asentado en tiempo las cancelaciones de una serie de deudas.

INFORME N°		EXPEDIENTE N°	
4101	2011	3030	2010

Montevideo, 10 de marzo de 2011.
Ref. Denuncia AA c/ Nuevo Banco Comercial S.A.

I. Antecedentes

1. El Sr. AA se presenta ante la Unidad Reguladora y de Control de Datos Personales, denunciando a BB S.A. por haber aportado información errónea en virtud de no haber asentado las cancelaciones de las deudas de que era titular.
Fue recibida vía correo electrónico con fecha 23 de septiembre de 2010 y presentada con firma y documentación adjunta, el 6 de octubre siguiente (fs. 1-49).
2. Se le confirió vista a BB con fecha 13 de octubre (fs. 60), quien la evacuó tempestivamente, el 26 de octubre (fs. 61-66). El 15 de noviembre se le dio traslado al denunciante (fs. 73), quien se presentó en tiempo y forma el 27 siguiente (fs. 74-77).
Con fecha 23 de diciembre de 2010, BB se notificó del informe N° 4900/2010 de 16 de diciembre de 2010 por el cual se le solicitaba: "proporcionar información acerca de cómo se generó la diferencia de U$S 48.94 y en su caso acredite la notificación de la deuda al Sr. AA. Asimismo se solicita se aclaren los motivos que ameritaron la comunicación a Clearing de Informes, con fecha 30/06/09, de una operación incumplida a cargo del Sr. AA, por el monto de US$ 570". Vencido con exceso el plazo para presentarse (fs. 86), BB no compareció.

II. Hechos Denunciados

1. El Sr. AA sostiene en lo medular que él y sus padres tomaron un préstamo amortizable con BB, pagadero en 23 cuotas trimestrales consecutivas de U$S 579.59, venciendo la primera de ellas el 31 de diciembre de 2003, por un monto de U$S 11.151,52.
Señala que en garantía del cumplimiento de ese préstamo, el denunciante constituyó derecho de prenda a favor de BB respecto de los certificados de depósitos de su propiedad, por un monto de U$S 12.126,29 y el plazo contractual fue fijado para el día que se cancelara la última cuota del préstamo tomado.

Afirma que en procura de su cancelación, autorizó a BB a que éste compensara los importes de las cuotas con el producido del certificado de depósito, con lo que la entidad bancaria se aseguraba el buen cobro de las sumas prestadas. Sin perjuicio de ello, frente a cada vencimiento, añade que su madre concurría a BB a depositar en efectivo y por ventanilla, el importe correspondiente a la diferencia entre el monto compensado y el valor de la cuota devengada (escasos dólares de diferencia entre el crédito y el débito). Así, como surge de la documentación agregada (fs. 18-47), se efectuaron todos y cada uno de los pagos por diferencias

en la propia sede bancaria.
En definitiva esgrime que a la fecha prevista para la cancelación de la deuda, en el mes de junio de 09, las partes nada debían a la institución bancaria.
2. Aduce que por sus actividades comerciales y personales, en noviembre de 2009 tomó conocimiento que en el mercado financiero, su categoría crediticia y la de sus padres, ante el BCU, era calificada con la categoría 5, es decir, deudor irrecuperable, incobrable.
Añade que tal calificación le significó que los Bancos de plaza con los cuales opera, automáticamente, por disposiciones del Regulador, lo catalogaran con categoría 3, es decir cliente con "capacidad de pago comprometida"; y como si ello fuera poco, fueron incluidos en CC con la operación incumplida.
3. Señala que pese a reiterados reclamos presentados ante el NBC, lo único que modificaron fue la inscripción ante CC, pero mantuvieron la nota ante el BCU.
Concluye manifestando que el manejo irresponsable de datos como el de obrados, al amparo de la normativa de protección de datos personales, debe ser considerado por el Órgano de Control, sancionando en caso de corresponder, a BB.

III. Argumentos de BB

1. BB, por su parte, sostiene que al vencer la última cuota de certificados de depósito en el mes de junio de 2009, el cliente depositó U$S 71.82. Sin embargo y en virtud del descalce que existía entre lo efectivamente percibido por el Banco en virtud de la prenda sobre certificados y la obligación mensual de pago de lo adeudado, se mantuvo una diferencia de U$S 48.94, a fin de poder cancelar totalmente el adeudo.
Afirma que esa circunstancia -de absoluta comprensión del Sr. AA en virtud de su calidad de ex empleado bancario- le fue informada por parte del Banco, negándose el deudor a concurrir a sus oficinas a efectos de cancelar dicho saldo. Añade que tal saldo deudor, conforme la normativa vigente del BCU debió ser informado por BB a la entidad reguladora, generándose en consecuencia el correspondiente registro negativo del deudor en dicha base. Manifiesta que la prueba de la existencia del crédito es que el Banco en ningún momento otorgó carta de pago por cancelación total y que obra en su poder el vale suscrito en su oportunidad, cuyo testimonio se acompaña. Establece que con referencia a la inscripción en CC, es política del Banco no mantener inscripciones en dicha base de datos por importes de poca cuantía como es el del Sr. AA y que la baja de la información no fue una acción puntual sino que se realizó dentro de un grupo de baja de registros de adeudos de similares características.
2. Señala que la legitimidad de su obrar quedará demostrada en el proceso jurisdiccional que iniciara el denunciante, mediante el diligenciamiento de los medios probatorios legalmente previstos y con todas las seguridades del debido proceso.

IV. Análisis

Violación a las disposiciones de la Ley N° 18.331

1. La Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (en adelante LPDP) consagra el derecho a la protección de datos personales como un derecho inherente a la persona humana a la vez que establece una serie de principios generales a los cuales debe sujetarse la actuación de los responsables de bases de datos, tanto públicos como privados y todos quienes actúen

con datos personales de terceros. (Artículos 1° y 5°)
El artículo 7° de la LPDP establece “Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones de la presente ley.
Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario. Cuando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley”.

La obligación contenida en el referido principio, impone la necesidad de que los datos personales que se recolecten en cualquier base de datos sean exactos y respondan, en todo momento, a la situación actual del titular, siendo el responsable de la base de datos quien debe velar por el cumplimiento de esta obligación.
Como expresa Lucrecio Rebollo, en el derecho español, comentando el principio de calidad de los datos, su exactitud y actualización “Se trata de un principio que afecta a la conservación del dato, que debe mantenerse siempre en perfecto estado con el fin de satisfacer las finalidades del tratamiento y no provocar, además, un perjuicio al interesado. La observancia de los principios de exactitud y actualización responde a la necesidad de trabajar con datos que revelen la situación presente y cierta del interesado, de manera que no se transformen en información inservible por su falsedad. Por otro lado, la inexactitud de un dato podría desligarle de la finalidad que legitimó su recogida, lo que deslegitimaría a su vez el tratamiento”. 1

Continúa diciendo el autor, analizando el artículo 4.4 de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal que si los datos fueran inexactos o incompletos, se cancelarán y se sustituirán de oficio por los datos en buen estado, sin que esto impida, en el mismo caso que recoge el precepto, el ejercicio por parte del interesado de los derechos de rectificación y cancelación.

2. Conforme surge de obrados, BB comunicó al Banco Central del Uruguay una deuda del denunciante que ameritó el mentado registro en CC, como deudor grado 5, irrecuperable.
Ahora bien, de acuerdo con la información y documentación aportada por el denunciante, éste canceló todas las obligaciones con BB en el mes de junio de 2009, constando agregados todos los recibos que acreditan que pagó todos los importes correspondientes a la diferencia entre el monto compensado y el valor de la cuota devengada (fs. 6 y 18-47).

Si bien NBC aduce que el registro negativo del Sr. AA en el BCU corresponde a que se mantuvo una diferencia de U$S 48.94 para poder cancelar totalmente el adeudo, no probó dicho extremo, como le fue solicitado por informe N° 4900/2010. Tampoco lo hizo en referencia a los motivos que ameritaron la comunicación a CC, con fecha 30/06/09, de una operación incumplida a cargo del Sr. AA, por el monto de U$S 570. (fs. 78 y 87).

1 REBOLLO DELGADO, Lucrecio; SERRANO PÉREZ, Ma. Mercedes; “Introducción a la Protección de Datos”, 2a. Edición, Editorial Dykinson, pág. 146

Adviértase sobre este aspecto que el Órgano de control puede solicitar, al amparo de lo previsto por el artículo 34, literal E) de la LPDP, información a entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran.

3. Tales hechos resultan contrarios al principio de veracidad supra aludido, en mérito a que el denunciado en calidad de acreedor comunicó datos a BCU de una deuda, que a la luz de la prueba incorporada resultaba saldada.

La LPDP atribuye la condición de responsable a la "persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento". (artículo 4°, literal K))
En cuanto al concepto de tratamiento de datos éste se define por el artículo 4°, literal M) como las "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"
Conforme lo relacionado, BB decidió sobre la finalidad, contenido y uso del tratamiento, comunicando al BCU una deuda saldada que ameritó la calificación del denunciante como deudor grado 5 en CC, información a la que pueden acceder terceras entidades para realizar una evaluación o perfil económico de las personas allí incorporadas.
En consecuencia, BB es responsable de que la información suministrada a BCU no responda al principio de veracidad recogido en el artículo 7° de la LPDP.

IV. Competencia de la URCDP

1. BB aduce que el Sr. AA, junto con sus padres lo citaron ante el Juzgado de Conciliación de 1er. Turno, previo al juicio por cobro de pesos emergentes de daños y perjuicios; y que la legitimidad del obrar de la entidad bancaria quedará demostrada en dicho proceso jurisdiccional mediante el diligenciamiento de los medios probatorios legalmente previstos y con todas las seguridades del debido proceso. (fs. 65).
Ahora bien, la Unidad Reguladora y de Control de Datos Personales, como Órgano de Control, debe velar por el cumplimiento de los objetivos y disposiciones de la LPDP. En ese marco, tiene entre otros cometidos el de asistir y asesorar a las personas que lo requieran acerca de los alcances de la Ley y el de imponer sanciones en caso que se violen las normas en ella establecidas (artículo 34, literal A) y 35 de la LPDP).
En mérito a ello, nada obsta -por el principio de independencia de jurisdicciones- que la URCDP asuma competencia en un asunto que es de su exclusivo resorte.

2. Por otra parte, el otorgamiento de garantías no es privativo de la órbita jurisdiccional, como parece entender el denunciado en su escrito a fs. 65.
En las presentes actuaciones se observaron las previsiones del Decreto 500/991, otorgándose a las partes oportunidad de formular descargos, presentar probanzas y ejercer su derecho de defensa. Fue el propio denunciado, en ese escenario, quien no realizó actuación alguna, tendente a comprobar que los datos comunicados a BCU, respondían al principio de veracidad supra aludido.

V. Potestad Sancionatoria

Conforme lo dispone la LPDP en su artículo 35, la URCDP podrá en ejercicio de sus potestades, aplicar a los infractores de las disposiciones de la Ley, las siguientes sanciones:

- Apercibimiento.
- Multa de hasta quinientas mil unidades indexadas.
- Promover ante los Órganos jurisdiccionales la suspensión de la base de datos respectiva.2

VI. Conclusiones

1. BB S.A. infringió el artículo 7° de la LPDP que regula el principio de veracidad de los datos, en tanto comunicó al Banco Central del Uruguay una deuda del Sr. AA que a la luz de la documentación aportada por éste, había sido cancelada en tiempo y forma, en el mes de junio de 2009.

2. Tal conducta infraccional se suma a la omisión de remitir la información que le requirió el Órgano de Control por informe N° 4900/2010, de 16/12/10 (fs. 78), del que fue notificado el 23/12/10 (fs. 86), al amparo de lo previsto por el artículo 35, literal E) de la LPDP.

3. Dicho extremo, sumado a que BB no registra antecedentes de infracciones anteriores y a que tiene en trámite de registro 11 bases de datos (Base de Depósitos SXXI, BANKTRADE COMEZ, COFRES, CRM, NODUM, INVERSIONES, TOPAZ TRACE, BUXIS, PUNTOS, BASE CENTRAL y AMEX), deberán ser tenidos en cuenta por el Consejo Ejecutivo de la URCDP, a los efectos de la graduación de la sanción a imponer.
Es todo cuanto tengo que informar.

Fdo. María José Rodríguez
Derechos Ciudadanos

2 La Ley N° 18.719, de Presupuesto Nacional, de 27 de diciembre de 2010, modificó dicha disposición, ampliando el elenco de sanciones, pero tal disposición es posterior al acaecimiento de los hechos. http://www.datospersonales.gub.uy/sitio/Leyes/ley-presupuesto-nacional.pdf.

Informe N° 5384 de 28 de abril de 2011.
Se informa denuncia por correo electrónico no deseado.

INFORME N°		EXPEDIENTE N°	
5384	2011	041	2011

Montevideo, 28 de abril de 2011.
Ref. Denuncia de Spam.

I. ANTECEDENTES

1. AA presenta denuncia de spam contra BB SC, en virtud de cuatro correos electrónicos no deseados recibidos en su casilla aa@cc.gub.uy.

2. Al evacuar la vista conferida, BB SC reconoce el envío, manifiesta que se trató de "un e-mail" remitido por error, y alega la inclusión en sus comunicaciones como mecanismo para evitar que los derechos de los receptores se vean afectados, la leyenda "Si recibe este mail por error, por favor, avise al remitente, luego de lo cual rogamos a Ud. destruya el mensaje original". Asimismo, expresa cumplir con todas y cada una de las obligaciones sustanciales y formales relativas a las bases de datos de las cuales es responsable y que las mismas se encuentran inscriptas ante esta Unidad.

3.La denuncia versa sobre la posible obtención y utilización de datos personales sin consentimiento de su titular, por lo que corresponde a la Unidad Reguladora y de Control de Datos Personales (URCDP) su sustanciación, en mérito a lo dispuesto en los artículos 34 y 35 de la Ley N° 18.331, de 11 de Agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data.

II. ANALISIS

A. GENERALIDADES

4. Spam. Definición. Problemática- "Se denomina Spam o "correo basura" a todo tipo de comunicación no solicitada, realizada por vía electrónica".31 Este tipo de comunicaciones tiene por finalidad la oferta, promoción y comercialización de productos, servicios y empresas.
Actualmente, y de acuerdo a la Directiva 2002/58/CE de la Unión Europea sobre la intimidad y las comunicaciones electrónicas, se recurre al concepto de correo electrónico comercial no solicitado como sinónimo de spam, definición continente de mensajes enviados por correo electrónico propiamente dicho (que utilizan el Protocolo SMTP), SMS (Short Message Service), MMS (Multimedia Messaging Service) y cualquier otra forma de comunicación aplicable.

Esta práctica se ha multiplicado en los últimos años debido a que su costo de utilización es muy bajo, a su velocidad y capacidad de volumen en las transmisiones, lo que se traduce en llevar una oferta rápidamente

3 Guía para la lucha contra el Spam. Agencia Española de Protección de Datos, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N-SPAM—ap-V.-30-mayo-cp-.pdf
.

a muchas personas de forma muy económica, a pesar de no haber sido solicitado por los destinatarios. Debido a ello, su utilización a más de ser abusiva e indiscriminada, vulnera derechos tales como los de la protección jurídica de los menores y la dignidad humana (cuando se difunden comunicaciones no aptas para menores o discriminatorias y racistas), los derechos de los consumidores (desde que no cumplen en absoluto con las leyes en la materia), el derecho a la intimidad (por ser intrusivo) y el derecho a la protección de datos (por utilizarse datos personales sin autorización de sus titulares).

4. Regulación.- Nuestro orden jurídico no cuenta con una normativa específica en materia de comunicaciones electrónicas no deseadas, pero sí cuenta con tutela constitucional y legal en materia de menores (Ley N° 17.823, de 7 de Setiembre de 2004, Código de la Niñez y la Adolescencia), dignidad humana (Art. 7, 72 y 332 de la Constitución de la República), derechos de los consumidores (Ley N° 17.250, de 11 de Agosto de 2000 de Defensa del Consumidor), derecho a la intimidad (Art. 7, 72 y 332 de la Constitución de la República) y protección de datos personales (Ley N° 18.331, de 11 de Agosto de 2008 de Protección de Datos Personales y Acción de Habeas Data). En este sentido, son erróneas las interpretaciones que entienden lícita esta práctica por falta de regulación.

Debemos tener presente que "Desde el punto de vista del individuo, el spam representa una intrusión en su intimidad. Esta consideración preside las nuevas normas sobre comunicaciones no solicitadas...".42 En sede de protección de datos y aplicado al caso que nos ocupa, el spam resulta violatorio desde que implica la obtención y utilización del dato personal correo electrónico sin consentimiento de su titular, según lo que se dirá.

6. Correo electrónico. Dato personal. Conforme viene de mencionarse de acuerdo con lo dispuesto en el artículo 4º literal D) de la Ley 18.331, el correo electrónico de la denunciante es un dato personal, puesto que se trata de información referida a una persona determinada, AA. Como tal, su tratamiento se encuentra sujeto al previo consentimiento informado de su titular, ya que en la especie y según se desprende de estas actuaciones, no resultan aplicables ninguna de las excepciones dispuestas en la citada norma.
B. BB SC

7. Error en el envío. Inexistencia.- BB SC reconoce haber enviado "un e-mail" pero alega error. Al respecto, esta informante entiende que asiste razón a la denunciante en sus descargos de fs. 25, en virtud que del expediente se desprende el envío de "cuatro correos consecutivos -tres de ellos con asunto y contenido diferentes- recibidos los días 3, 9, 17 y 23 de Marzo de 2011 (fs. 1, 3, 5 y 11)". Situación que despeja toda duda sobre un error aislado y hace presumir que el correo de presunción que no fuera controvertida por prueba en contrario. Asimismo, se corrobora que los contenidos refieren a cursos ofrecidos por la denunciada y que ninguno de los cuatro correos posee la leyenda alegada por la misma, situaciones que refuerzan la hipótesis de encontrarnos ante una práctica de spam.

4 "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones no solicitadas o spam. Comisión de las Comunidades Europeas, Bruselas, 22.01.2004 COM (2004) 28 final". Disponible sobre https://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/COMUNICACION-COM-28.pdf

8. Consentimiento de AA. Inexistencia.- No resulta probado en las presentes actuaciones que la denunciante hubiese consentido el tratamiento de su correo electrónico a fin de recibir ofertas sobre cursos impartidos por BB SC.

Ningún documento ha sido presentado al efecto, por lo que deberá presumirse que el mismo no fue prestado. Reafirma lo expresado, el hecho que nuestra norma rectora en materia de protección de datos no acepte el consentimiento tácito -a diferencia de legislaciones comparadas-, erigiendo como régimen general el consentimiento expreso y documentado.

9. Falta de registro de Bases de Datos.- En sus descargos, la denunciada manifiesta que las bases de datos de las cuales es responsable se encuentran inscriptas ante esta Unidad, lo que no es correcto. BB SC comenzó el proceso de inscripción ingresando la información on line, pero no lo culminó. Por ende, BB SC no posee resolución de inscripción de sus Bases de Datos los que las torna ilegales al tenor de lo dispuesto en el artículo 6º inciso primero de la Ley N° 18.33154. En consecuencia, carece en absoluto de sustento el argumento de la denunciada de cumplir con todas y cada una de las obligaciones sustanciales y formales relativas a las bases de las cuales es responsable, desde que una base ilegal no puede garantizar ningún derecho a los titulares de datos.

III. CONCLUSIONES

1. La consulta planteada refiere al tratamiento del dato personal correo electrónico de AA sin su consentimiento para el envío de comunicaciones electrónicas no solicitadas (spam), por lo que se encuentra alcanzado por la Ley Nº 18331, de Protección de Datos Personales y Acción de Habeas Data y su Derecho reglamentario.

2. Se constató el envío desde la casilla dail@bb.com reconocida por la denunciada como propia, a la casilla aa@cc.com.uy de la denunciante, de cuatro correos electrónicos consecutivos no solicitados, conteniendo información sobre cursos dictados por BB SC, y que ninguno de los cuatro correos posee la leyenda alegada por la misma, lo que excluye cualquier hipótesis de error en el proceder de la denunciada y hace presumir que el correo de la denunciante forma parte de una base de datos utilizada por BB SC, presunción que no fuera controvertida por prueba en contrario y sustenta por ende la hipótesis de encontrarnos ante una práctica de spam.

3. No se probó en las presentes actuaciones que la denunciante hubiese consentido el tratamiento de su correo electrónico a fin de recibir ofertas sobre cursos impartidos por BB SC. Por lo que deberá presumirse que el mismo no fue prestado.

4. Las bases de datos responsabilidad de BB SC no se encuentran inscriptas ante esta Unidad, por lo que son ilegales al tenor de lo dispuesto en el artículo 6º de la Ley N° 18.331 y consecuentemente inhábiles para garantizar los derechos de los titulares de los datos.

5. Atento a lo expuesto, considerando la primariedad en la infracción cometida y en función de lo preceptuado

5 3. "Principio de legalidad.- La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia".

en los artículos 6º, 9º y 35 de la Ley N° 18.331, este último en su redacción dada por el artículo 152 de la Ley N° 18.719 de 27 de Diciembre de 2010, se recomienda la aplicación de una observación a BB SC intimándosele conjuntamente a la culminación del proceso de registro de sus bases de datos en el plazo de 30 días corridos.
Es todo cuanto tengo que informar.

Fdo. Bárbara Muracciole
Derechos Ciudadanos

Informe N° 5615 de 9 de mayo de 2011.

Se informa denuncia en relación con la forma de actuación de la Unidas Reguladora y de Control de Datos Personales (URCDP) vinculada con la información de las empresas amparadas por el secreto profesional en el marco de las inspecciones que se realicen.

INFORME N°		EXPEDIENTE N°	
5615	2011	052	2011

Montevideo, 9 de mayo de 2011.
Ref. Consulta sobre cómo va a proceder la URCDP c/ la información de las empresas amparadas por el secreto profesional.

I – CONSULTA

La consulta es a propósito de las bases de datos pertenecientes a Asesores de Inversión, cuya operativa profesional incluye la recolección y tratamiento de datos personales de sus clientes.
Estos clientes son inversores efectivos o potenciales a los que sus Asesores les prestan un servicio caracterizado como de aproximación o intermediación (actividades de corretaje en definitiva), hacia fuentes radicadas en el país o en el exterior, para colocar capitales o realizar otro tipo de negocios.

Se consulta en concreto para este tipo de responsables "si amparados en el Secreto Profesional, cumpliendo con la inscripción de las Bases de Datos relacionadas a la actividad y permitiendo ejercer a los titulares de datos todos los derechos que la normativa consagra, es posible resguardar la confidencialidad de los datos frente a una inspección... [de la URCDP] en base al régimen de secreto en virtud de la actividad que desempeñan".

II – FACULTADES DE FISCALIZACIÓN E INSPECCIÓN DE LA URCDP

El art. 34 lit. D) de la Ley Nº 18.331, en su redacción actual dada por el art. 155 de la Ley Nº 18.719, establece y precisa una serie de facultades en favor de la URCDP, para el desenvolvimiento de sus cometidos de fiscalización e inspección de las bases de datos personales sometidas a su control.

Entre dichas facultades se encuentran las de exigir a responsables y encargados la exhibición de todo tipo de documentación, tradicional o digital, intervenir el material inspeccionado, tomar medidas de seguridad para su conservación pudiendo copiarlos, incautar tales elementos en situaciones graves hasta por seis días hábiles prorrogables por la Justicia si fuera imprescindible, y requerir informaciones a terceros.
A mayor abundamiento la misma norma establece la posibilidad de acudir al auxilio de la fuerza pública y la orden judicial de allanamiento.
La citada normativa tiene su fuente de inspiración en disposiciones similares que rigen para las

administraciones tributarias (art. 68 del Código Tributario), adaptadas a las competencias específicas de la URCDP.

III – RESPUESTA A LA CONSULTA FORMULADA

Si la ley le concedió a la URCDP las facultades examinadas, es porque entiende pertinente y procedente que las lleve a cabo con éxito, en cabal cumplimiento de sus competencias y funciones de contralor. El mismo razonamiento ha sido empleado, a nuestro entender con justeza, en el ámbito tributario, del cual -por razones antes anotadas- cabe extraer inspiración para aplicarla en la sede que nos ocupa: "La Administración goza de las más amplias facultades de investigación y fiscalización, a los efectos de la determinación de la obligación tributaria. Esas facultades se consagran en una norma de rango legal que establece un principio general del actuar de la Administración, cumpliéndose con lo preceptuado por el artículo 7º de la Constitución (ley formal y material dictada en razón del interés general); no puede sostenerse que se vulnere el mencionado secreto a menos que exista un texto expreso que limite las mencionadas atribuciones".6

No obstante es del caso advertir que el tema no está zanjado, existiendo posturas discrepantes en la doctrina nacional tributarista1, que sostienen prácticamente la inexpugnabilidad del secreto profesional como parte del sistema esencial de garantía de los derechos fundamentales7.

Ciertamente estamos en presencia, como en tantos otros ámbitos, de situaciones donde debe aplicarse el juicio de razonabilidad o ponderación, para arribar a la mejor forma de lograr el mínimo sacrificio del conjunto de derechos y deberes en juego. Sin que ello oculte la dificultad y singularidad de cada caso.

Sobre tal problemática y su dificultad se ha expresado con agudeza y abundancia conceptual RODRÍGUEZ VILLALBA, al considerar que "ciertos sectores profesionales pueden disponer de informaciones decisivas por su calidad, abundancia, exactitud o relación directa con las situaciones subjetivas que se indagan. Nuevamente los valores jurídicos individualistas, derivados del derecho a la seguridad e intimidad de la personal, requieren compatibilizarse con el interés público." Y agrega el mismo autor: "Es obvio que la regulación jurídica debe contemplar equitativamente ambas exigencias.

Pero esta conclusión evidente plantea dificultades de concreción, pues el límite de hasta dónde es posible ampliar el área de las potestades de los organismos administrativos y hasta dónde debe mantenerse intangible la esfera del secreto es decididamente incierto. No es posible definir una orientación unívoca en el Derecho Tributario, aunque la tendencia de las legislaciones positivas insinúa el decaimiento condicionado de este deber."8

6 1. Pronunciamiento de la Sala de Profesionales de la Dirección General Impositiva sobre Administración Tributaria: Facultades y Alcances" Publicado en Revista Tributaria tomo XXXIII Nº 191 mar-abr 2006 págs. 267-277.

7 2. Gianni GUTIÉRREZ PRIETO y Alberto VARELA RELLÁN - "El Contribuyente frente a la Inspección Fiscal", de. AMF, 2007, 413 ps.; Raúl D´ALESSANDRO - "Allanamiento y vulneración del secreto profesional. ¿Facultades de la Administración Tributaria?, en Revista Tributaria Tomo XXXII Nº 185 mar-abr 2005 págs. 222-24.

8 Gustavo RODRÍGUEZ VILLALBA - "Las facultades de la Administración en los procedimientos de determinación tributaria" en

Por lo tanto, a la luz de las dificultades y divergencias expuestas, se aconseja como regla preservar el secreto profesional sobre las informaciones objeto de inspección o fiscalización, y solamente ceder o exceptuar de dicha regla aquellos casos en que irremediablemente se frustraría la probanza o cautela perseguidas. Merced a tal designio es de orden concluir que las facultades de la Administración deberán ser ejercitadas con mesura y raciocinio, buscando evitar o minimizar lo más posible la colisión con otros derechos y o deberes fundamentales.

La disponibilidad de este tipo de informaciones puede resultar esencial o no para el éxito de la medida. Dependerá de las singularidades de cada caso, y de la dinámica que adquiera la medida de inspección o fiscalización una vez en curso de ejecución. Dependerá así de las contingencias que se presenten, sin desmedro de la necesidad de una fundamentada, cuidadosa y bien estudiada planificación de tales medidas, de forma anticipada a llevarlas a cabo.

Regirá, asimismo, el principio de economía de medios, la cual deberá ser medida en todo momento en función de los resultados perseguidos. Solamente agotadas otras posibilidades, y si se entendiera absolutamente necesario para el éxito de la medida, estará justificado avanzar hacia el conocimiento de la información que se entiende sometida a secreto profesional. No se admite lo que en ámbitos tributaristas se denomina (y tampoco se le consiente a la Administración si lo intenta) la “expedición de pesca”.

Vulgarmente reconocible como “tirar para recoger”. La inspección y/o fiscalización deben ser certeras y objetivas. Los casos dudosos, o bien se deben resolver durante el transcurso de la propia labor inspectiva o fiscalizadora buscando fórmulas que preserven el secreto profesional (ej. solicitando la desagregación de este tipo de información del material inspeccionado o fiscalizado), o bien requerirán de una orden judicial, que justifique el levantamiento del secreto imperante para poder actuar con propiedad.
En todos estos casos, cualquiera sea el resultado final de estas labores de control administrativo, se deberá preservar el derecho de defensa y de contradictorio del sujeto inspeccionado o fiscalizado, buscando su máxima colaboración consentida por escrito.

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Revista Tributaria Nº 141 nov-dic 1997 págs. 765-809.

Informe N° 5643 de 11 de mayo de 2011.

Se informa consulta de videovigilancia efectuada por la Dirección Nacional de Casinos.

INFORME N°		EXPEDIENTE N°
5643	2011	2011-2-10-0000098

Montevideo, 11 de mayo de 2011.
Ref. Consulta de la Dirección Nacional de Casinos.

-I- Antecedentes

El 25 de abril de 2011, la Dirección General de Casinos formula ante la Unidad Reguladora y de Control de Datos Personales (en adelante URDCP), consulta referente a la videovigilancia en las diferentes Salas de Juego y aplicación de la normativa vigente en materia de protección de datos personales, en los siguientes términos:

1.- Conforme al literal K) del artículo 4º de la Ley 18.331, con referencia a las Bases de Datos, dispone que: "Responsable de la base de datos o del tratamiento: persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento". - ¿Es correcto interpretar, a los efectos de su inscripción, que el responsable de las bases del Organismo es el Director General de Casinos?
- Conforme al literal H) de la citada norma, "Encargado del tratamiento: 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": - ¿Es correcto interpretar que el Director General de Casinos, aún cuando delegue en Gerentes de Salas o Casinos y en el Departamento de Circuitos Cerrados de Televisión, siempre será él el responsable de las Bases de Datos?

2.- Teniendo en cuenta el tipo de equipamiento y las limitaciones del mismo, con el que cuenta el Departamento de Circuitos Cerrados de Televisión, ¿cuál sería la opción correcta a tomar en caso de brindar acceso a un interesado (titular de los datos) a grabaciones con su imagen, dado que se estaría exhibiendo, en la mayoría de los casos, imágenes de otras personas de las cuales no se tiene su consentimiento para ello, teniendo en cuenta que nuestros equipos no tienen una tecnología que permita ocultar la fisonomía de cada uno de ellos?.- En tal caso, de negarse a brindar esa información al titular de los datos, para proteger la identidad de otras personas, ¿se estaría incumpliendo la Ley?

A su vez, en la referida consulta se aclara a tales efectos que la "La Dirección General de Casinos es una Unidad Ejecutora del Ministerio de Economía y Finanzas, que tiene a su cargo la explotación de juegos de azar de casinos, en Salas de Juego instaladas en 17 departamentos del país. Al frente de dichos establecimientos se encuentran Gerentes o funcionarios que desempeñan ese rol, designados por la autoridad competente".

-II- Análisis del alcance de los términos "responsable" y "encargado de tratamiento".

Efectivamente tal como se expresa en la consulta, el literal K) del artículo 4º de la Ley 18.331, dispone que el responsable de la base de datos o del tratamiento es la persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

A su vez, el art. 12 establece que por el Principio de Responsabilidad, el responsable de la base de datos será responsable de la violación de las disposiciones de la ley.

Por último en el art. 35 se establece que el órgano de control, podrá aplicar medidas sancionatorias a los responsables de las bases de datos o encargados del tratamiento de datos personales en caso que se violen las normas previstas en la misma.

En tanto, en la guía para el llenado de formularios de inscripción elaborada por la URCDP9 se establece que se deberán "indicar los datos del titular o representante de la Base de Datos o del tratamiento. El responsable es la 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 el caso de empresas privadas, se señalarán los datos del o los representantes estatutarios. En el caso de Organismos Públicos se detallarán los datos del Jerarca correspondiente. En caso que éste sea Colegiado quien lo represente" (subrayado nuestro).

Por su parte, también la Agencia Española de Protección de Datos (AEPD), en la Guía para Responsable de Ficheros10, establece que "El responsable de un fichero o tratamiento es la entidad, persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales.

A su vez, el Grupo del Artículo 29 sobre Protección de Datos11 (G29), en el Dictamen 1/2010 sobre los términos "responsable del tratamiento" y "encargado del tratamiento", indica que "El concepto de responsable del tratamiento es autónomo, (...) y funcional, en el sentido de que su objetivo es asignar responsabilidades en función de la capacidad de influencia de hecho, y, por consiguiente, se basa en un análisis de los hechos más que en un análisis formal".

Este grupo de trabajo en función de ello establece que hay tres componentes a tener en cuenta, entre ellos el aspecto personal ("la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo"), la posibilidad de un control plural ("que solo o conjuntamente con otros") y los elementos esenciales para distinguir al responsable del tratamiento de otros agentes ("determine los fines y los medios del tratamiento de datos personales").

9 Página web de la URCDP www.datospersonales.org.uy/registros. Vista 29 de marzo de 2011.

10 Guía del responsable de ficheros. AEPD
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf.
Vista 2 de abril de 2011.

11 Grupo creado en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad. Sus cometidos se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. Sitio web: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

En cuanto al concepto de encargado del tratamiento, establecen que su "existencia depende de una decisión adoptada por el responsable del tratamiento, que puede decidir que los datos se traten dentro de su organización o bien delegar todas o una parte de las actividades de tratamiento en una organización externa".
En el Dictamen se realizan una serie de consideraciones que apuntan a reconocer la importancia de poder diferenciar entre responsable y encargado de tratamiento en virtud de que al delimitar el alcance del término responsable se puede determinar "quién debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera los interesados pueden ejercer sus derechos en la práctica. En otras palabras, debe asignar la responsabilidad".
Concluyen que, "el elemento más importante es el que establece que el encargado del tratamiento actúa "por cuenta del responsable del tratamiento". Actuar en nombre de alguien significa servir los intereses de otro y remite al concepto legal de "delegación".

-III-"Responsable" y "Encargado de Tratamiento" en el ámbito de la Dirección General de Casinos

De la información disponible en el sitio web del organismo consultante sus competencias específicas incluyen:
1. Gestionar y operar directamente los juegos de Azar de Casinos y Salas de Esparcimiento.
2. Contribuir a la recaudación estatal en forma directa.
3. Complementar las inversiones de origen privado en materia turística y/o comercial en los sectores de interés nacional y/o departamental, con la explotación directa de Juegos de Azar de Casinos y Salas de Esparcimiento.

Se informa también, que a efectos de la explotación directa por parte del Estado de una Sala de Esparcimiento, la Dirección General de Casinos se encuentra facultada a disponer su apertura conforme lo dispuesto en la legislación vigente (artículo 31 del Decreto Nº 284/1998, de 14 de octubre de 1998).

Los objetivos estratégicos de la Dirección General de Casinos incluyen también, la complementación por parte de este Organismo, de las inversiones de origen privado en el sector turístico, con la explotación directa por parte del Estado de Juegos de Azar de Casinos y Salas de Esparcimiento.
También dentro de sus cometidos se encuentra la detección del juego ilícito, el que se encuentra previsto como una falta en el Código Penal.

De la información descripta surge que la DGC tiene cometidos específicos, regulados como tal en la legislación vigente en la materia.
Por ende, respecto a la pregunta de si ¿Es correcto interpretar, a los efectos de su inscripción, que el responsable de las bases del Organismo es el Director General de Casinos? La respuesta debe ser afirmativa en función de que es el jerarca de esta dirección quien decide sobre la finalidad, contenido y uso del tratamiento de sus bases de datos.

En cuanto a la segunda interrogante: - ¿Es correcto interpretar que el Director General de Casinos, aún

cuando delegue en Gerentes de Salas o Casinos y en el Departamento de Circuitos Cerrados de Televisión, siempre será él el responsable de las Bases de Datos? La respuesta debe ser afirmativa ya que tanto los Gerentes de Salas o Casinos, como el Departamento de Circuitos Cerrados de Televisión, tratan los datos en nombre del responsable de dichas bases de datos.

En definitiva, de acuerdo al análisis jurídico realizado respecto de los términos "responsable" y "encargado de tratamiento", así como de los cometidos específicos que posee la Dirección consultante, cabe concluir que el jerarca de la misma es quien debe representar al organismo obligado o responsable en los términos y alcance previstos en la norma, aunque delegue en diferentes encargados de tratamientos según corresponda, ya sean Gerentes de Salas o Casinos, o en el Departamento de Circuitos Cerrados de Televisión.

-IV-Sobre el ejercicio del derecho acceso por parte de los titulares de los datos contenidos en la base
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP), se expidió al respecto mediante el Dictamen N° 10, de 16 de abril de 201012, estableciendo entre otras consideraciones, que a la videovigilancia es aplicable la normativa de protección de datos personales cuando se utilicen cámaras o cualquier otro medio análogo que capte, trate, registre o almacene imágenes que refiera a personas identificadas o identificables.

Agrega que en la videovigilancia deben observarse los principios de la protección de datos ( ) entre ellos el principio de legalidad por lo cual el tratamiento debe ser lícito, se debe verificar que la videoviglancia cumple con la normativa vigente, acorde con lo cual resulta necesaria la inscripción de las Bases de Datos ante el Registro de Base de Datos Personales a cargo de esta Unidad de conformidad con la LPDP y sus decretos reglamentarios".
Asimismo establece que "los responsables de las Bases de Datos de videovigilancia deben cumplir con determinadas obligaciones:

a. Ser responsables por el cumplimiento de la normativa que los regula, sobre todo en lo referido a la protección de datos personales.

b. Actuar con la debida reserva o sea adoptar medidas de seguridad para garantizar que solamente las personas autorizadas accedan a la Base de Datos.

c. Mantener la información en forma confidencial, por la cual el responsable debe ser el custodio de las imágenes.

d. Garantizar que el titular de los datos pueda ejercer su derecho de acceso.

e. Proceder al registro de las correspondientes Bases de Datos así como informar a las personas que sus imágenes están siendo captadas(subrayado nuestro).

12 Dictamen de la URCDP sobre Videovigilancia
http://www.datospersonales.gub.uy/sitio/dictamenes.aspx
Página visitada 10 de mayo de 2011.

A la luz del referido dictamen, es claro que a las bases de datos producto de la videovigilancia se les aplica la normativa vigente en materia de protección de datos personales, y que además, entre las obligaciones que tienen los responsables de dichas bases, está la de garantizar el ejercicio del derecho acceso. El problema es cómo garantizar este derecho sin vulnerar derechos de terceros.

Al respecto la Agencia Española de Protección de Datos (AEPD) en el Informe Jurídico 0193/2007 13, Ejercicio de derechos en Videovigilancia, establece que(...) el acceso que se efectúe no puede implicar una violación a los derechos de terceros, por tanto ( ) el responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento".

Establece esta Agencia, que esa medida asegura el equilibrio entre ambos derechos, esto es atender el acceso y no comunicar datos de terceros. No obstante se podrá optar por otros medios iguales de efectivos, siempre que dicho equilibrio se mantenga.

También la Agencia Española de Protección de Datos en su Guía sobre Videovigilancia14, concluye que "el ejercicio de los derechos posee perfiles específicos en el ámbito de la videovigilancia", y agrega que "el ejercicio del derecho de acceso reviste características singulares:
1. Requiere aportar como documentación complementaria una imagen actualizada que permita al responsable verificar y contrastar la presencia del afectado en sus registros.
2. Resulta prácticamente imposible acceder a imágenes sin que pueda verse comprometida la imagen de un tercero. Por ello puede facilitarse el acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento. Ej. "Su imagen fue registrada en nuestros sistemas el día ___ del mes del año entre las _ horas y las _ horas. En concreto el sistema registra su acceso y salida del edificio.
Si se ejerciese el derecho de acceso ante el responsable de un sistema que únicamente reproduzca imágenes sin registrarlas deberá responderse en todo caso indicando la ausencia de imágenes grabadas."

-V-Conclusiones

A) El Director de la Dirección General de Casinos es el responsable de la base de datos de videvigilancia en los términos y alcance previstos en la Ley N° 18.331 y su Decreto reglamentario, aunque delegue en diferentes encargados de tratamientos según corresponda, ya sean Gerentes de Salas o Casinos, o en el Departamento de Circuitos Cerrados de Televisión.

---

13 Agencia Española de Protección de Datos (AEPD). Informe jurídico 0193/2007. Ejercicio de derechos en Video Vigilancia: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2007-0193_Videovigilancia.-Ejercicio-de-derechos..pdf. Página visitada el 9 de mayo de 2011.

14 Agencia Española de Protección de Datos. Guía Videovigilancia. (AEPD) http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf. Página visitada el 9 de mayo de 2011
.

B) A efectos de cumplir con la ley se deberá garantizar el ejercicio del derecho de acceso (art. 14), dando respuesta por escrito al solicitante, dentro del plazo previsto en la Ley y detallando la información existente en la referida base sobre su persona, sin vulnerar derechos de terceros.

Fdo. Dra. Graciela Romero
Derechos Ciudadanos

Informe N° 5674 de 26 de mayo de 2011.
Se informa denuncia por correo electrónico no deseado.

INFORME N°		EXPEDIENTE N°
5674	2011	2011-2-10-0000335

Montevideo, 26 de mayo de 2011.
Ref. Denuncia de Spam.

I. ANTECEDENTES

1. AA presenta denuncia de spam contra Renglón Uno, en virtud de correo electrónico no deseado recibido en su casilla personal aa@adinet.com.uy.

2. En su mérito, se confirió vista a BB quien al evacuarla, reconoció como forma habitual de divulgar sus cursos el envío de correos electrónicos. Explica que los mismos se encuentran contenidos en dos bases compuestas por datos sobre ex alumnos, personas que solicitaron información sobre capacitaciones, además de información relevada de sitios web, diarios, revistas, guías, listados de asociaciones, de cámaras empresariales y sectoriales, de empresas, de asociaciones de profesionales y de órganos públicos. Manifiesta asimismo, que sus comunicaciones cuentan con la opción para que el destinatario pueda darse de baja. Por último, expresa que no puede responder en qué base de datos se encuentra la denunciante por la reserva de su identidad.

3. Debido a la referida reserva, se confirió vista a la denunciante de lo manifestado por BB solicitándole autorización para revelar su correo electrónico. Habiendo vencido el plazo conferido sin respuesta, debe interpretarse que la denunciante deniega la autorización pedida.

4. La denuncia versa sobre la posible obtención y utilización de datos personales sin consentimiento, por lo que corresponde a la Unidad Reguladora y de Control de Datos Personales (URCDP) su sustanciación, en mérito a lo dispuesto en los artículos 34 y 35 de la Ley N° 18.331, de 11 de Agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data.

II. ANÁLISIS

A. GENERALIDADES

5. Spam. Definición. Problemática- “Se denomina Spam o “correo basura” a todo tipo de comunicación no solicitada, realizada por vía electrónica”.151 Este tipo de comunicaciones tiene por finalidad la oferta, promoción y comercialización de productos, servicios y empresas.
Actualmente, y de acuerdo a la Directiva 2002/58/CE de la Unión Europea sobre la intimidad y las comunicaciones electrónicas, se recurre al concepto de correo electrónico comercial no solicitado como

15 Guía para la lucha contra el Spam. Agencia Española de Protección de Datos, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N-SPAM—ap-V.-30-mayo-cp-.pdf.

sinónimo de spam, definición continente de mensajes enviados por correo electrónico propiamente dicho (que utilizan el Protocolo SMTP), SMS (Short Message Service), MMS (Multimedia Messaging Service) y cualquier otra forma de comunicación aplicable.

Esta práctica se ha multiplicado en los últimos años debido a su bajo costo de utilización, a su velocidad y a su capacidad de volumen en las transmisiones, lo que se traduce en llevar una oferta rápidamente, a muchas personas, de forma muy económica, a pesar de no haber sido solicitado por los destinatarios. Debido a ello, su utilización a más de ser abusiva e indiscriminada, vulnera derechos tales como los de la protección jurídica de los menores y la dignidad humana (cuando se difunden comunicaciones no aptas para menores o discriminatorias y racistas), los derechos de los consumidores (desde que no cumplen en absoluto con las leyes en la materia), el derecho a la intimidad (por ser intrusivo) y el derecho a la protección de datos (por utilizarse datos personales sin autorización de sus titulares).

6. Regulación.- Nuestro orden jurídico no cuenta con una normativa específica en materia de comunicaciones electrónicas no deseadas, pero sí cuenta con tutela constitucional y legal en materia de menores (Ley N° 17.823, de 7 de Setiembre de 2004, Código de la Niñez y la Adolescencia), dignidad humana (Art. 7º, 72 y 332 de la Constitución de la República), derechos de los consumidores (Ley N° 17.250, de 11 de Agosto de 2000 de Defensa del Consumidor), derecho a la intimidad (Art. 72 y 332 de la Constitución de la República) y protección de datos personales (Ley N° 18.331, de 11 de Agosto de 2008 de Protección de Datos Personales y Acción de Habeas Data). En este sentido, son erróneas las interpretaciones que entienden lícita esta práctica por falta de regulación.

Debemos tener presente que "Desde el punto de vista del individuo, el spam representa una intrusión en su intimidad. Esta consideración preside las nuevas normas sobre comunicaciones no solicitadas ...".162 En sede de protección de datos y aplicado al caso que nos ocupa, el spam resulta violatorio desde que implica la obtención y utilización del dato personal correo electrónico sin consentimiento de su titular.

7. Correo electrónico. Dato personal.- Conforme viene de mencionarse y de acuerdo con lo dispuesto en el artículo 4º literal D) de la Ley N° 18.331173, el correo electrónico es un dato personal, puesto que se trata de información referida a una persona física o jurídica determinada o determinable. Como tal su tratamiento se encuentra sujeto al previo consentimiento informado de su titular, salvo las excepciones dispuestas en la citada norma.

16 2 "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones no solicitadas o spam. Comisión de las Comunidades Europeas, Bruselas, 22.01.2004 COM (2004) 28 final". Disponible sobre https://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/COMUNICACION-COM-28.pdf

17 3 "Definiciones.- A los efectos de la presente ley se entiende por: D) Dato personal: información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables".

Si bien la denunciante no autorizó la revelación de su identidad y respecto de la misma no es posible determinar la licitud en el envío de comunicaciones electrónicas por parte de BB, de los descargos del denunciado se desprenden irregularidades que fundamentan la prosecución de estas actuaciones, según se dirá.

8. Desconocimiento de la Ley. Falta de registro.- BB manifiesta desconocer la Ley N° 18.331, lo que en forma alguna resulta una excusa admisible para el incumplimiento de la norma en general y para la falta de registro de las bases de datos de las cuales es responsable, en particular 184. Por otra parte, la referida falta de registro no se condice con el manejo responsable de los datos alegado por el denunciado en sus descargos, desde que las bases de datos no inscriptas son ilegales al tenor de lo dispuesto en el artículo 6º inciso primero de la
Ley N° 18.331195 y por ende inhábiles para garantizar el ejercicio de los derechos de sus titulares.
Asimismo, de los descargos presentados, se advierte la existencia de más bases de datos que las declaradas. En efecto, el denunciado reconoce ser responsable de dos bases de datos las cuales, por las descripciones vertidas, corresponden a las denominadas "Base de Clientes" y "Base de Datos Públicos" cuyo proceso de inscripción se iniciara ante esta Unidad con posterioridad a tomar vista de las presentes actuaciones. Sin embargo, del escrito presentado por el denunciado, surge claramente la existencia de al menos otra base de datos responsabilidad de BB: su equipo docente. Ello se desprende de las expresiones vertidas a fs. 22 en cuanto a que "contamos con un equipo docente de reconocida trayectoria y gran experiencia en las áreas temáticas que les toca desarrollar. (Adjunto CV de los docentes)." La información organizada sobre el capital humano empleado por particulares o empresas, tan detallada como la de los currículos agregados, constituye una base de datos conforme las definiciones de la Ley N° 18.331206.

9. Consentimiento. Falta de prueba.- BB admite que divulga sus cursos únicamente por vía electrónica, por lo que reconoce que utiliza el dato personal correo electrónico de variadas personas. Del mismo modo, manifiesta que posee dos bases continentes de dichos correos que ha "construido a través de los años", que se componen "en una gran parte de datos de ex-alumnos y de personas que han solicitado información sobre capacitaciones" y "... de direcciones electrónicas extraídas exclusivamente de fuentes públicas, como sitios web, diarios, revistas, guías, listados de asociaciones, listados de cámaras empresariales, listados de cámaras sectoriales ..." entre otras.
No obstante, BB no ha probado en estas actuaciones que los titulares de los datos hubiesen consentido el tratamiento de su correo electrónico a fin de recibir ofertas sobre los cursos que imparte.

---

18 4 Artículo 2 del Código Civil "La ignorancia de las leyes no sirve de excusa"

19 5 "Principio de legalidad.- La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia".

20 6 Artículo 4 literal A) "Base de datos: 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".

Ningún documento ha sido presentado al efecto, ni ninguna excepción normativa ha sido invocada, por lo que deberá presumirse que el mismo no fue prestado. Reafirma lo expresado, el hecho que nuestra norma rectora en materia de protección de datos no acepte el consentimiento tácito -a diferencia de legislaciones comparadas-, erigiendo como régimen general el consentimiento expreso y documentado.
Otro elemento a tener en cuenta, resulta de las expresiones del denunciado al referir como públicas una variedad de fuentes, confundiendo el canal o instrumento de publicidad con la fuente en sí misma, tal es el caso de los "sitios web" que menciona. Situación que hace suponer que recaba información sin autorización de sus titulares aún cuando la misma debiera ser requerida. Téngase presente que en todos los casos y según sus propias expresiones, nos encontramos ante la utilización de un dato que de principio requiere el previo consentimiento informado, salvo las excepciones previstas en la norma de Protección de Datos que no fueron invocadas.

III. CONCLUSIONES

1. La denuncia planteada refiere al tratamiento del dato personal correo electrónico sin consentimiento, para el envío de comunicaciones electrónicas no solicitadas (spam), por lo que se encuentra alcanzada por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data y su Decreto reglamentario.

2. Si bien la denunciante no autorizó la revelación de su correo electrónico y respecto de la misma no es posible determinar si se configuró el envío de comunicaciones electrónicas no solicitadas por el denunciado, de los descargos presentados se desprenden irregularidades que fundamentan la prosecución de estas actuaciones, las que se mencionan a continuación.

2.1 Las bases de datos responsabilidad del denunciado no se encuentran inscriptas ante esta Unidad, por lo que son ilegales al tenor de lo dispuesto en el artículo 6º de la Ley N° 18.331 y consecuentemente inhábiles para garantizar los derechos de los titulares de los datos, configurando un incumplimiento inobjetable a la referida norma.

2.2 De los descargos presentados se advierte la existencia de más bases de datos que las declaradas.

2.3 BB no ha probado en las presentes actuaciones que los titulares de los correos electrónicos que admite utilizar, hubiesen consentido el tratamiento a fin de recibir ofertas sobre los cursos que imparte. Ningún documento ha sido presentado al efecto, ni ninguna excepción normativa ha sido invocada, por lo que deberá presumirse que el mismo no fue prestado.

3. Atento a lo expuesto, considerando la primariedad y en función de lo preceptuado en los artículos 6º, 9º y 35 de la Ley N° 18.331, este último en su redacción dada por el artículo 152 de la Ley N° 18.719, de 27 de Diciembre de 2010, se recomienda la aplicación de una observación a BB, intimándosele conjuntamente al registro de todas las bases de datos de las que sea responsable, en el plazo de 30 días corridos.

Se adjunta versión sin los datos de la denunciante en caso de solicitarse copia por el denunciado.
Es todo cuanto tengo que informar.

Fdo. Bárbara Muracciole
Derechos Ciudadanos

Informe N° 5934 de 3 de junio de 2011.

Se informa consulta relativa a la posibilidad de utilizar el número de cédula de identidad del usuario para acceder a consultas en línea relativas a los servicios que presta Obra Sanitarias del Estado (OSE).

INFORME N°		EXPEDIENTE N°
5934	2011	2011-2-10-0000171

Montevideo, 3 de junio de 2011.
Ref. Consulta de OSE.

-I-Antecedentes

La presente consulta fue formulada por las Obras Sanitarias del Estado (O.S.E), a través del Sr. Enrique Balestrino, integrante de la comisión multidisciplinaria que pretende adecuar y alinear el Organismo a las Leyes Nos. 18.331 y 18.381, de Protección de Datos Personales y Acción de Habeas Data, y de Acceso a la Información Pública, respectivamente.
En lo medular expresan que siguiendo los criterios y lineamientos de AGESIC y en procura de brindar servicios enmarcados en el Gobierno Electrónico, se encuentran abocados a la mejora de trámites de gestión y consulta al ciudadano usuario de los servicios de agua potable y saneamiento, con el fin de facilitar la realización de gestiones comerciales a través de la Web, esto es, a través del Portal de OSE.

Entre las distintas gestiones que puede realizar el usuario, se encuentra la de acceso a su cuenta (por ej. para acceder al duplicado de la factura). Ello implica el ingreso del número de cuenta del usuario, pero como no siempre el usuario tiene disponible en el momento de la consulta su número de cuenta, se establece como forma de ingreso alternativa, el dato personal de la cédula de identidad.

En definitiva, solicitan se les informe si es válido el acceso por documento de identidad, aún si ese dato conduce a datos que pueden ser privados, a efectos de establecer un equilibrio entre favorecer los trámites de forma electrónica y proteger los datos personales.

-II-Análisis

1. Competencia de la Unidad Reguladora y de Control de Datos Personales (URCDP).
El órgano de control tiene potestades para expedirse sobre la consulta de marras, en virtud de los cometidos atribuidos por el artículo 34 de la Ley Nº 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (en adelante LPDP).

2. Disposiciones de la LPDP aplicables.
El sistema de gestión y consulta instaurado por OSE implica un tratamiento de datos en los términos

establecidos por el artículo 4º literal M) de la LPDP, en tanto lo define como las "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".
El mismo artículo, en su literal D) define dato personal como "información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables".
El número de cédula de identidad en tanto puede determinar a una persona, es un dato personal.
Por su parte, el artículo 9° que prevé el principio del previo consentimiento informado, consagra que el tratamiento de datos personales será lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado. Añade dicha disposición que no será necesario dicho consentimiento cuando:

A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.

B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

E) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico.
Asimismo, el artículo 7º de la LPDP que regula el principio de veracidad de los datos, limita la recolección y el tratamiento de éstos a aquellos que revistan ciertas particularidades en relación con la finalidad para la cual hayan sido obtenidos. Esto es, que sean veraces, adecuados, ecuánimes y no excesivos.
Según el diccionario de la Real Academia Española, veraz refiere a la verdad; adecuado a lo apropiado a las condiciones, circunstancias u objeto de algo; ecuanimidad a imparcialidad de juicio; y excesivo, que excede y sale de la regla.
Si analizamos las acepciones en sentido global, extraemos que, en todo caso, los datos personales que sean objeto de tratamiento y se incorporen a una base de datos, deben ser realmente apropiados para la finalidad buscada. Deben mantener estricta conexión con el resto de los datos incorporados a la base de datos, pero además, y aunque resulten pertinentes por su naturaleza, debe ser absolutamente necesaria su inclusión en relación con la finalidad a la que se destina. 21

3. Pertinencia de la incorporación de la cédula de identidad al sistema de gestión y consulta.
Ahora bien, las disposiciones analizadas, a la luz del sistema de gestión y consulta del Portal de OSE indican que no sería recomendable la incorporación del dato personal cédula de identidad del usuario para acceder a la información que el Organismo brinda al usuario.

21 REBOLLO, Lucrecio, SERRANO, Ma. Mercedes, "Introducción a la Protección de Datos", a. Edición 2008, Madrid, pág. 144-145
.

En efecto, cualquier persona que conozca el número de cédula de identidad de otra, podrá acceder fácilmente a la factura del consultado, tomando conocimiento del nombre completo del titular del servicio, domicilio, tipo de tarifa de que se trata (familiar u otro), unidad, así como el detalle del consumo con el monto a pagar y deudas si las tuviere.
Para una efectiva constatación de ello, se accedió al sitio web http://www.ose.com.uy/ pestaña "Servicios en línea" http://www.ose.com.uy/c_servicios_en_linea.html, "Iniciar gestión comercial". Allí, se indica que se podrá ingresar por "Número de cuenta que figura en su factura" o "Documento de identidad del titular del contrato". Se agregan las páginas web, debidamente certificadas.

-III- Conclusiones

En virtud de lo expuesto y en opinión de esta informante, el número de cedula de identidad se erige en el presente caso como un dato excesivo para la finalidad buscada, cual es en todo caso promover políticas de Gobierno Electrónico, permitiendo al ciudadano la realización de gestiones a través de la Web a fin de que conozca el detalle del servicio contratado asociado a sus datos personales, acceda al duplicado de factura correspondiente y realice otras gestiones que considere necesarias referidas a tal servicio.

En razón de ello, la identificación de usuario del sistema que no merece reparos desde el punto de vista de la normativa de protección de datos personales (LPDP y Decreto reglamentario N° 414/009, de 31 de agosto de 2009) es el otro dato que figura en la página web: "Número de Cuenta".

Dicho dato, que naturalmente solo puede conocer el titular del servicio, a la luz de la normativa examinada constituye un dato pertinente y no excesivo con la finalidad buscada.
Es todo cuanto tengo que informar.

Fdo. Dra. María José Rodríguez
Derechos Ciudadanos

Informe N° 6010 de 9 de junio de 2011.

Se informa consulta de la Dirección Nacional de Asistencia y Seguridad Social Policial respecto de las condiciones en que se debería relacionar ésta con el Banco de Previsión Social.

INFORME N°		EXPEDIENTE N°
6010	2011	2011-2-10-0000072

Montevideo, 9 de junio de 2011.
Ref. Consulta de asesoría jurídica de la Dirección Nacional de Asistencia y Seguridad Social Policial

- I -LA CONSULTA

Se consulta por parte de la Asesoría Jurídica de la Dirección Nacional de Asistencia y Seguridad Social Policial del Ministerio del Interior, respecto del marco jurídico, limitaciones o condiciones legales, que regulan el relacionamiento de esa repartición con el Banco de Previsión Social para llevar a cabo el sistema de liquidación de jubilaciones y pensiones policiales, a propósito del régimen de protección de datos personales.

A mayor precisión, la consultante expresa que "a un año ya de la implementación del nuevo sistema informático a través de la empresa (…) también suministradora al BPS del sistema de liquidación de jubilaciones y pensiones mensual, es que surgieron requerimientos por parte de nuestra Institución, tales como la necesidad de contar con un Web Service donde consultar la base de datos de nuestras pasividades y sus núcleos familiares, con fines estadísticos de políticas sociales y de control de derecho a fin de evitar pagar beneficios dobles (ej. asignaciones familiares). Resulta que la base de datos en los hechos es compartida. De ahí la disyuntiva de brindar datos que en opinión del BPS, en principio no sería viable en virtud de la ley de protección de datos personales". (fs. 2)

- II - ANTECEDENTES NORMATIVOS

La Dirección Nacional de Asistencia y Seguridad Social Policial (D.N.A.S.S.P.) fue creada por el Decreto Ley Nº 14.230 con los cometidos de dirigir, coordinar y supervisar las actividades de varios servicios, entre ellos el "Servicio de Retiros y Pensiones Policiales" y el "Servicio de Tutela Social Policial" (art. 2º que modifica la Sección VIII art. 21 de la Ley Orgánica Policial, ordenada por Decreto Nº 75/972 según Leyes Nros. 13.963 y 14.050, de 22 de mayo de 1971 y 23 de diciembre de 1971, respectivamente).

Desde su creación esta Dirección ha funcionado en coordinación con el Banco de Previsión Social, previéndose un régimen de transición (arts. 3º y 4º de la misma norma), pasaje de expedientes y demás documentos (art. 6º), asistencia técnica y administrativa a solicitud del Servicio (art. 7º), y pasaje del "Fondo de Seguro de Vida e Invalidez y Gastos de Sepelio" bajo el nombre de "Fondo de Tutela Social Policial" al Servicio de Tutela Social Policial (art. 8º).

El 22 de julio de 2004 se suscribió Convenio entre los Organismos agregado a este expediente, de cuyo tenor surgen lineamientos de cooperación para el "intercambio de información técnico-profesional en el área de seguridad social en general" (cláusula segunda apartado "A") así como los tipos de datos personales sujetos a intercambio (Anexo I).

Por Ley Nº 18.405m de 24 de octubre de 2008 se reorganiza el sistema previsional policial, estableciéndose entre otros aspectos que "la gestión del sistema estará a cargo del Servicio de Retiros y Pensiones Policiales, subordinado a la Dirección Nacional de Asistencia y Seguridad Social Policial" (art. 3º primera frase).

El 24 de febrero de 2010 se suscribe un Convenio de Cooperación Interinstitucional entre el Ministerio del Interior y la D.N.A.S.S.P. y el Banco de Previsión Social que también obra agregado al expediente, para la reingeniería de los procesos informáticos de la D.N.A.S.S.P., en el marco de cooperación entre Organismos del Estado y, específicamente, de la reforma previsional antes referida.

- III - APLICACIÓN DE LOS ARTS. 157 A 160 DE LA LEY Nº 18.719 SOBRE INTERCAMBIO DE INFORMACIÓN ENTRE ORGANISMOS PÚBLICOS

El intercambio de información entre organismos públicos se rige actualmente por los arts. 157 a 160 de la Ley Nº 18.719, de 27 de diciembre de 2010, siendo particularmente aplicables al caso los siguientes preceptos:

Art. 157.- Las entidades públicas, estatales o no, deberán adoptar las medidas necesarias e incorporar en sus respectivos ámbitos de actividad las tecnologías requeridas para promover el intercambio de información pública o privada autorizada por su titular, disponible en medios electrónicos.

Art. 158.- Son obligaciones de las entidades públicas, estatales o no:

…

B) Los sujetos involucrados en el intercambio deberán cumplir con las obligaciones de secreto, reserva o confidencialidad. Asimismo, adoptar aquellas medidas necesarias para garantizar niveles de seguridad y confidencialidad adecuados.

C) Recabar el consentimiento de acuerdo con lo previsto en la Ley número 18331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Hábeas Data.

Art. 159.- A los efectos de cumplir con los cometidos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, en el intercambio de información las entidades públicas, estatales o no, deberán ajustar su actuación a los siguientes principios generales:

A) Cooperación e integralidad.

B) Finalidad.

C) Confianza y seguridad.

D) Previo consentimiento informado de los titulares de los datos personales.

E) Eficiencia y eficacia.

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

La reglamentación establecerá el mecanismo para proceder al intercambio de información. Sin perjuicio de ello, el procedimiento se iniciará con la presentación de una solicitud fundada y firmada por el jerarca del organismo emisor, ante el jerarca del organismo receptor.
Cuando proceda el intercambio de información, los organismos podrán:

1) Formalizar un acuerdo que establezca los mecanismos o condiciones de intercambio.

2) Adoptar los mecanismos o condiciones de intercambio definidos por el órgano competente y formalizar un acuerdo.
En ambos casos, el acuerdo establecerá las condiciones, protocolos y criterios funcionales o técnicos con los que se llevará a cabo dicho intercambio.

- IV - APLICACIÓN DE LOS ARTS. 9 LIT. B) Y 17 LIT. B) DE LA LA LEY Nº 18.331

Se aplican al caso igualmente los arts. 9º lit. B) y 17 lit. B) de la Ley Nº 18.331, a saber, que regulan algunas de las hipótesis donde se faculta a prescindir del consentimiento del interesado para el tratamiento y comunicación de sus datos personales, conforme citamos a continuación:
Art. 9… 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.
Art. 17… El previo consentimiento [para la comunicación] no será necesario cuando:
…
B) en los supuestos del artículo 9º de la presente ley.

- V - ANÁLISIS Y CONCLUSIONES

1.- El intercambio de información y la interoperabilidad entre organismos públicos es de principio, por lo que debe primar un criterio básico de apertura y aceptación, desde luego sin excluir ni atemperar el cumplimiento de todas aquellas medidas adecuadas (legales y técnicas) que permitan llevarlo a cabo bajo cánones respetuosos de todo el sistema jurídico, en particular preservando el derecho fundamental a la protección de datos personales (Ley Nº 18.331 y arts. 157 a 160 de la Ley Nº 18.719).

2. De acuerdo a los términos de la consulta así como lo que surge de la documentación cuya agregación se solicitara, el planteo de la consultante merece una respuesta afirmativa bajo las prevenciones antedichas.

3. Se agrega a lo ya concluido, las siguientes razones puntuales al caso:

A) La aspiración de disponer de la información que hoy no tiene, tal cual fuera expuesta por la consultante, obedece a una necesidad fundada en razones objetivas de servicio: compartir un cierto conjunto de datos de los afiliados, que actualmente están en poder exclusivo de uno de los organismos involucrados en el sistema de retiros y pensiones policiales (el Banco de Previsión Social), para así poder cumplir con su rol singular dentro del referido sistema previsional sectorial de origen legal.

B) Avala lo expresado la propia documentación suscrita entre ambos organismos que luce agregada al

expediente (“Convenio de Cooperación Interinstitucional para la Reingeniería de la D.N.A.S.S.P....”), cuya cláusula 11 alude con precisión a la tipología de datos objeto de necesario intercambio, mientras que la cláusula 12 se remite expresamente al amparo de los artículos 9º, lit b) y 17 lit. b) de la Ley Nº 18.331. Con lo cual queda claro que ambas partes reconocieron en su oportunidad la pertinencia y legitimidad de este intercambio.

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 6039 de 13 de junio de 2011.

Se informa consulta del Fondo de Solidaridad respecto si puede informar o no la identidad de los beneficiarios de las becas.

INFORME N°		EXPEDIENTE N°
6039	2011	2011-2-10-0000180

Montevideo, 13 de junio de 2011.
Ref. Consulta formulada por el Fondo de Solidaridad.

-I- Antecedentes

El Fondo de Solidaridad consulta a la Unidad Reguladora y de Control de Datos Personales si conforme las disposiciones de la Ley Nº 18.331, de Protección de Datos Personales y Acción de Habeas Data (LPDP) se encuentra habilitado a informar la identidad de los beneficiarios de las becas que otorga la Institución y si la Universidad de la República y UTU pueden proporcionarle los datos que permitan localizar a los egresados de dichos entes de enseñanza.

-II- Argumentos

1. Sobre la posibilidad de informar la identidad de los becarios, luego de efectuar un análisis de la normativa que les aplica, indican que la situación les genera dudas en virtud de la Ley de Protección de Datos Personales.
Sostienen que en el caso se contrapone el principio de transparencia de la gestión pública con el derecho a la protección de datos personales de los becarios.

2. Sobre la posibilidad de que la Universidad de la República y UTU proporcionen los datos de localización de los egresados señalan:

a) Que existen razones de hecho que justifican la comunicación de datos. Afirman que si la Ley Nº 16.524 asigna al Fondo de Solidaridad la facultad de recaudar el tributo e impone a los entes de enseñanza el deber de enviar información de los egresados, lo mismo comprende la información de al menos el domicilio o el teléfono de dichos contribuyentes, única forma de poder comunicar la existencia de adeudos, intimar las sumas adeudadas y adoptar medidas tendientes al cumplimiento coactivo de la prestación.

b) Que la información que sería proporcionada -crucial para la recaudación y fiscalización del tributo- es la que permite ubicar al contribuyente, esto es, además de su nombre, carrera cursada y fecha de egreso (datos que se proporcionan actualmente), la dirección, e-mail o teléfono de dicho contribuyente. No se solicita información protegida por el secreto estadístico (Ley Nº 16.616), la que además no reviste ningún interés para la Institución.

c) Que el proporcionar los datos aludidos se enmarca en el deber impuesto a los entes de enseñanza por

el artículo 9º de la Ley Nº 16.524, ya que la no inclusión de dichos datos vuelve inútil la información que pueda proporcionarles la Universidad de la República. En consecuencia, sería de aplicación el artículo 9º de la Ley Nº 18.331 que excepciona del principio del previo consentimiento informado a aquellos datos que "Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".

-III- Análisis

1. Cometidos asignados al Fondo de Solidaridad (FDS).
La Ley Nº 16.524, de 25 de julio de 1994 crea el Fondo de Solidaridad como persona jurídica de derecho público no estatal, el que será organizado y administrado por una Comisión Honoraria integrada por siete miembros, con el cometido de financiar un sistema de becas para estudiantes de la Universidad de la República y de UTU.

El FDS se integra mediante una contribución especial (artículo 13 del Código Tributario) efectuada por los egresados de las Instituciones mencionadas, cuyos ingresos mensuales sean superiores a cuatro salarios mínimos nacionales, la que se abonará a partir de cumplido el quinto año del egreso, hasta completar veinticinco años de aportes al FDS o hasta que se efectivice el cese en la actividad laboral por jubilación.
El artículo 9º de la norma referida, impone a la Universidad de la República y a la Administración Nacional de Educación Pública, el deber de enviar a la Comisión Honoraria, dentro de los primeros treinta días de cada año, la nómina completa de quienes hayan obtenido títulos profesionales, lo que es reiterado por el artículo 9º del Decreto 325/002, reglamentario de la Ley Nº 16.524.

2. Sobre la posibilidad de que la Universidad de la República (UdelaR) proporcione al FDS los datos de localización de los egresados.
El FDS pretende por parte de la UdelaR una comunicación de datos, definida por la LPDP como "toda revelación de datos realizada a una persona distinta del titular de los datos".
Ahora bien, como lo prevé el artículo 17 de la LPDP "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".
Dicha disposición se ve complementada, por lo previsto en el artículo 9°de la LPDP que excepciona del previo consentimiento al titular cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal (literal B)).

La Ley Nº 16.524 en su artículo 9º impone a la UdelaR y a la UTU, el envío a la Comisión del FDS, en los primeros treinta días de cada año, de la nómina completa de quienes hayan obtenido títulos profesionales comprendidos en la ley durante el año inmediato anterior y la fecha exacta de expedición. Asimismo, exige que la UdelaR proporcione también a la Comisión del FDS, la información registrada en el Servicio Central de Bienestar Universitario, a fin de coordinar el cumplimiento de la Ley.

Es decir que dicha disposición legal, exime del previo consentimiento al titular de los datos, pero en todo caso tal comunicación lo será para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario, por expreso mandato legal (artículo 17 LPDP).
Ahora bien, la Ley Nº 16.524 alude anómina completa lo que está indicando nombres y apellidos de los egresados, no así datos de localización como pretende el FDS (dirección, e-mail o teléfono del contribuyente).

Sobre este aspecto le asiste razón al consultante en el sentido que el no contar con datos identificatorios resulta un impedimento para poder comunicar la existencia de adeudos, intimar las sumas adeudadas y adoptar medidas tendientes al cumplimiento coactivo de la prestación. Es decir, cumplir con el objetivo esencial de Ley Nº 16.524, cual es la concesión de becas para cuya financiación es estrictamente necesario la recaudación del tributo.
En mérito a ello, corresponde analizar qué tipo de datos podrían ser adecuados y no excesivos en relación con la finalidad para la que se destinan, conforme lo previsto por el artículo 7º de la LPDP.
Esta disposición contempla la necesidad de que el tratamiento y/o comunicación de un determinado dato personal, deba ser proporcional a la finalidad que lo motiva.

En mérito a lo expuesto y atendiendo al cometido específico que ostenta el FDS, sería pertinente de acuerdo con el principio de finalidad, que la UdelaR y la ANEP- Consejo de Educación Técnico Profesional (UTU) comuniquen al FDS además de los nombres y apellidos de egresados, fechas de egreso y carreras asociadas, el domicilio de áquellos.

Y ello, en atención a las disposiciones legales citadas, que se complementan con lo previsto por el literal C) del artículo 9º de la LPDP que contempla al domicilio como un dato que no requiere el consentimiento del titular para su tratamiento y/o comunicación.

3. Sobre la posibilidad de informar la identidad de los becarios.
El FDS expresa que en la operativa diaria de la Institución, es muy común que los estudiantes o quienes se acercan a sus oficinas pregunten a los funcionarios si tal o cual persona es beneficiario de la beca, creándose muchas veces la disyuntiva si debe primar el principio de transparencia de la gestión pública, o el derecho a la protección de datos personales de los becarios.

El Fondo de Solidaridad es una persona jurídica de derecho público no estatal (artículo 1º Ley Nº 16.524) y por tanto le aplican las disposiciones de la Ley Nº 18.381, de Acceso a la Información Pública, de 7 de octubre de 2008 y de su Decreto reglamentario Nº 232/010, de 2 de agosto de 2010.

En la presente hipótesis estamos en presencia de dos derechos fundamentales. Por un lado el derecho a la protección de los datos personales que consiste en el poder de disposición y de control sobre ellos, que se concreta en la facultad de consentir su recolección, la obtención y acceso, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular; y el derecho de acceso a la información pública que implica en puridad la facultad que ostenta cualquier ciudadano de

acceder a toda la información que se halle en poder del Estado, en sentido amplio, para así ejercer un poder de controlar en el manejo de los recursos que en definitiva pertenecen a toda la sociedad.

En razón de ello corresponde realizar una ponderación de ambos derechos, atendiendo fundamentalmente al cumplimiento de la finalidad perseguida en el tratamiento de los datos de los becarios.
La LPDP delimita una serie de principios generales que trazan el tratamiento de los datos personales por parte de los responsables de bases de datos o encargados de tratamiento y que sirven como instrumento interpretativo para resolver las cuestiones que pueden suscitarse en la aplicación de las disposiciones de la Ley. (artículo 5º, in fine). Tales principios deberán observarse durante toda la vida del dato, desde su recolección, hasta su cancelación o eliminación.

Entre ellos se encuentra el de finalidad, verdadera piedra angular en la protección de los datos personales, que establece que los datos objeto de tratamiento no podrán utilizarse para finalidades distintas o incompatibles con áquellas que motivaron su obtención.

Conforme lo dispuesto por los artículos 2º y 7º de la Ley Nº 16.524, la finalidad del tratamiento de los datos por parte del Fondo de Solidaridad es el procesamiento de la información de los estudiantes a fin de determinar si cumplen o no las condiciones legales para ser becarios, es decir si carecen de recursos económicos suficientes.
En razón de ello, los contribuyentes que concurren al financiamiento del sistema y la sociedad toda, ostentan el derecho a tomar conocimiento de las personas a quienes se proporcionan las becas, a fin de poder ejercer, de ese modo, un poder de contralor de la gestión de la Institución.
Ello no implica que la entidad consultante deba publicar la información a través de su sitio web, sino que ante una solicitud individualizada o genérica se cumpla con informar la identidad de dichos beneficiarios.

-IV-Conclusiones

1. Conforme las disposiciones de la LPDP analizadas a la luz de los cometidos asignados por Ley al Fondo de Solidaridad, la Universidad de la República y la ANEP- Consejo de Educación Técnico Profesional (UTU) podrían legítimamente comunicarle a aquél, además de la nómina de egresados, fecha de egreso y carrera asociada, el domicilio del contribuyente.

2. En cuanto al punto objeto de consulta que refiere a la posibilidad de informar la identidad de los becarios, realizando una ponderación de los derechos en juego, a la luz del principio de finalidad, se estima que procede la divulgación de la identidad de los beneficiarios de las becas, ante una solicitud individualizada o genérica.
Es todo cuanto tengo que informar.

Fdo. Dra. María José Rodríguez
Derechos Ciudadanos

Informe N° 6090 de 20 de junio de 2011.
Se informa consulta de Carrasco Lawn Tennis relativa a la posibilidad de entregar el padrón social a requerimiento de los socios.

INFORME N°		EXPEDIENTE N°
6090	2011	2011-2-10-0000193

Montevideo, 20 de junio de 2011.
Ref. Consulta Carrasco Lawn Tennis Club.

-I-Antecedentes

La presente consulta viene a consideración de la Unidad Reguladora y de Control de Datos Personales (URCDP) en virtud de la consulta formulada por el Carrasco Lawn Tennis Club (CLTC) acerca de si resulta ajustada a derecho la entrega de copias de su padrón social, a requerimiento de sus socios.
CLTC aduce que tales solicitudes responden a diferentes motivos, entre otros para ser utilizados en actos electorales internos de la Institución.

Señala que en virtud de que el padrón social se conforma de sendos datos personales, a efectos de evitar abusos con los eventuales datos obtenidos se entendió no brindarlos sin el expreso consentimiento de los involucrados, en el marco de lo dispuesto por el artículo 72 de la Constitución de la República y de lo previsto por el artículo 9º de la Ley Nº 18.331.

-II-Análisis

1. Objeto de consulta – Comunicación de datos.- Conforme lo relatado, se pretende por parte del CLTC una comunicación de datos personales.
Dato personal, de acuerdo con lo dispuesto por el artículo 4° literal D) de la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (en adelante LPDP) es “información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables”.
Comunicación de datos, por su parte, es definida por la misma norma, en su literal B) como “toda revelación de datos realizada a una persona distinta del titular de los datos”.
Para que esa comunicación de datos sea legítima conforme con la LPDP, deben cumplirse los requisitos contemplados el artículo 17 que refieren, con carácter general, al cumplimiento de los fines directamente relacionados con los intereses legítimos de emisor y destinatario, siempre que se cuente con el consentimiento de los titulares de los datos.

Es decir que el artículo 17 exige de modo expreso dos requisitos conjuntos: interés legítimo de emisor y destinatario y previo consentimiento del titular (requisito de índole complejo, atento a que además de

documentarse el consentimiento deberá informársele finalidad de la comunicación y destinatario).

2. Excepciones al consentimiento.- La norma excepciona del previo consentimiento cuando:
- lo disponga una ley de interés general,
- en los supuestos del artículo 9°,
- se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, emergencia, para realizar estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos,
- se trate de datos disociados.

3. Caso concreto.- En la presente hipótesis no se verifican los requerimientos contemplados en la disposición legal.
En efecto, el interés legítimo solo podría vislumbrarse desde la órbita del destinatario (socio de la Institución), pero no del emisor, que en principio no lo moviliza ningún interés ni simple ni cualificado.
La ausencia de este requisito, por sí solo bastaría para desestimar la pretensa comunicación de datos, no obstante procederemos a examinar las excepciones dispuestas en la norma.
El artículo 9º de la LPDP, al que remite el artículo 17 exime del deber de recabar el previo consentimiento informado en los siguientes supuestos:

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

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

C) 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 para las personas jurídicas, razón social, nombre de fantasía, RUT, domicilio, teléfono e identidad de las personas a cargo de la misma;

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

E) Cuando se realice por personas físicas para su uso exclusivo, personal o doméstico.
Las restantes hipótesis contempladas en los literales c) y d) del artículo 17 (datos relativos a la salud y datos disociados), no se aplican en la especie.

4. Conclusiones preliminares.- De las normas analizadas, los únicos supuestos que podrían tener cabida para legitimar una comunicación de datos sin consentimiento del titular podrían ser los contemplados en los literales C), D) y E) del artículo 9º.
No obstante:
- En la hipótesis del literal D) solo sería legítima una comunicación de datos si en los Estatutos del CLTC se prevé tal posibilidad y dicho extremo es de conocimiento del socio.
- La hipótesis precedente, así como las previstas en los literales C) y E) no deben interpretarse descontextualizadas de todo el elenco normativo de la LPDP, fundamentalmente de los principios generales que la regulan, verdaderos pilares de la protección de datos personales.

En efecto, el artículo 8º que regula el principio de finalidad de los datos, estatuye que los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con áquellas que motivaron su obtención.
Ello implica que el socio cuando se afilió a la Institución aportó datos personales para una finalidad específica, circunscripta al ámbito del CLTC.

Por tanto y salvo el caso que en los estatutos o en la ficha de afiliación se detalle expresamente la posibilidad de comunicación de datos a otros socios, para finalidades específicas (por ej. en el marco de actos eleccionarios), se deberá recabar el consentimiento informado del socio para legitimar la cesión de datos que se pretende.
Dicho consentimiento no será válido si la información que se facilita al titular no le permite conocer la finalidad a que se destinarán los datos comunicados o la actividad de la persona a la que se pretende comunicar. (artículo 13 de la LPDP)

-III -Conclusión general

Conforme las disposiciones de la LPDP analizadas supra, a la luz de la información aportada por la consultante, no resulta ajustado a derecho que CLTC comunique datos personales de sus socios, a otros socios que lo hayan requerido, sin el consentimiento informado de áquellos.
Es todo cuanto tengo que informar.

Fdo. Dra. María José Rodríguez
Derechos Ciudadanos

Informe N° 6201 de 4 de julio de 2011.

Se informa denuncia por inclusión múltiple en una base de datos de morosos.

INFORME N°		EXPEDIENTE N°
6201	2011	2011-2-10-0000155

Montevideo, 4 de julio de 2011.
Ref. Denuncia de AA c/ BB.

-I-Antecedentes

La presente viene a consideración de la Unidad Reguladora y de Control de Datos Personales (URCDP) en virtud de la denuncia formulada por el Sr. AA contra BB, por inclusión múltiple ante CC.

-II-Hechos denunciados

1. El Sr. AA sostiene que por una deuda contraída con su tarjeta de crédito del Banco BB se le registra como deudor en CC con fecha 25 de marzo de 2000. Añade que posteriormente se inicia gestión de cobro por parte de Banco BB y se le incluye nuevamente por la misma deuda con fecha 6 de noviembre de 2002 y luego una tercera vez, con fecha 22 de noviembre de 2002, contraviniendo de esa forma los plazos máximos de registro pautados por la normativa vigente.

2. Solicitada información por parte de la URCDP, el Sr. AA contesta el 6 de junio de 2011, expresando que la deuda no ha sido cancelada y reafirma la ilicitud de registro del antecedente más allá de los 10 años.
Se otorga vista a las entidades involucradas, BB y CC a fin de que se expidan sobre la legitimidad del registro de la deuda y su plazo, conforme lo previsto por el artículo 22 de la Ley Nº 18.331, de 11 de agosto de 2011, de Protección de Datos Personales y Acción de Habeas Data (LPDP).

-III- Argumentos de las partes

1. Luego de haberse notificado las vistas correspondientes a CC y BB, con fechas 13 de junio y 15 de junio de 2011, respectivamente, el 17 de junio, el Sr. AA envía a la dirección electrónica de contacto de la URCDP infourcdp@agesic.gub.uy un correo en el que manifiesta que el objeto de la denuncia contra BB respecto a la inclusión múltiple, ha sido resuelto en forma satisfactoria, para lo cual adjunta comunicado enviado por CC.

2. CC y BB evacuan en tiempo y forma las vistas conferidas.

2.1. CC aduce que una vez denunciada y planteada la situación directamente ante sus oficinas por parte del Sr. AA, procedieron a actualizar (cancelar) y suprimir (retirar) la información que se encontraba figurando en la base de datos a nombre del denunciante. Agrega que el Sr. AA ya ha sido informado de ello, tal cual se demuestra con el mail adjunto.
En virtud de ello, solicita se archiven las presentes actuaciones.

2.2. BB, por su parte, indica que igual solicitud que la formulada por la URCDP al otorgarle vista, fue planteada por el propio denunciante Sr. AA ante el Banco Central del Uruguay y evacuada por BB., con fecha 21 de junio de 2011, como surge de la nota adjunta como Anexo B.
En dicha respuesta, BB manifiesta que "…en virtud de que su deuda generada por Tarjeta … fue oportunamente vendida a Fideicomiso …, le hemos solicitado a dicha empresa la baja de la inscripción ante CC, dado que la deuda originalmente fue ingresada en el año 2000, la cual caducó automáticamente al cumplir los 10 años".

-IV-Análisis

1. Competencia del Órgano de Control.- La URCDP tiene competencia para expedirse en los presentes obrados, en mérito a lo dispuesto por la LPDP en su artículo 34 literal A) que le asigna el cometido de asistir y asesorar a las personas que lo requieran acerca de los alcances la Ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.

2. Objeto de la Denuncia.- Según surge de las presentes actuaciones, el Sr. AA tenía ante CC diversos asientos como titular de una única deuda, con fechas que excedían el plazo previsto legalmente. Situación que objetivamente considerada violentaría, en principio, las previsiones contenidas en los artículos 7º y 22 de la LPDP, que regulan el principio de veracidad y los datos relativos a la actividad comercial o crediticia, respectivamente.

En efecto, el artículo 7º estatuye que los datos deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido; que deberán ser exactos y actualizarse en el caso en que ello fuere necesario; y finalmente, cuando se constate inexactitud o falsedad, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados y que deberán eliminarse áquellos que hayan caducado, de acuerdo a lo previsto en la LPDP.

El artículo 22 ordena que los datos personales relativos a obligaciones de carácter comercial de personas físicas solo podrán estar registrados por un plazo de cinco años contados desde su incorporación y que si al vencimiento de dicho plazo la obligación permanece incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años.

En el presente caso, como surge del expediente electrónico, el denunciante formuló reclamo a través del "contáctenos" de la web de BB, especificando la situación que lo perjudicaba, con fecha 30/04/11, reclamo No. SN- 002332. (vide folio No. 5 del expediente electrónico)
Sin embargo, fue recién luego de su acercamiento ante CC, el 14 de junio de 2011, que ante comunicación de ésta con la empresa afiliada BB, se realiza la correspondiente rectificación del registro.
Efectivamente, como surge del correo electrónico adjunto de CC (folio 62 del expediente electrónico), "En virtud de su visita a nuestra oficina el día 14 de junio del corriente, habiéndonos puesto en conocimiento de la situación por usted detallada, procedimos al estudio del caso. Se reclamó a la empresa afiliada el envío inmediato de la cancelación de fecha 6 de junio del corriente, la cual a partir de ayer figura en la categoría

"operaciones canceladas con atraso. Por otra parte, se solicitó rectificación de la situación relativa a un mismo incumplimiento registrado en el año 2000 y 2002, el cual por tener mínimas diferencias de importe y fechas, había sido admitido por el sistema. La empresa afiliada solicitó el retiro de esos incumplimientos, procedimos a su retiro sin dejar ningún tipo de antecedentes".

De todo lo expuesto se constata que la situación denunciada por el Sr. AA fue solucionada, procediéndose a realizar las cancelaciones y rectificaciones correspondientes, tal como surge de los propios dichos del denunciante y de las empresas involucradas.
Ahora bien, tal como se expuso en párrafos precedentes, BB tomó conocimiento del hecho objeto de denuncia, a través del contacto de su página Web el 30 de abril de 2011 (folio 5). Sin embargo, se procedió a la efectiva rectificación del error en el mes de junio, tal como surge de lo relatado por CC y de la comunicación cursada al denunciante por parte de BB con fecha 21 de junio de 2011 (folio 72), extremo que a la luz de lo previsto por el artículo 15 de la LPDP ameritaría la imposición de sanción, conforme lo dispuesto en el mismo cuerpo normativo, artículo 35.

Tengamos presente que la obligación contenida en el principio regulado en el ya citado artículo 7° de la LPDP, impone la necesidad de que los datos personales que se recolecten en cualquier base de datos sean exactos y respondan, en todo momento, a la situación actual del titular, siendo el responsable de la base de datos quien debe velar por el cumplimiento de esta obligación.

Por su parte, el artículo 15 de la LPDP establece que los titulares de datos pueden ejercer los derechos de rectificación, actualización, inclusión o supresión ante los responsables de bases de datos y éstos tienen la obligación de proceder a la rectificación actualización, inclusión o supresión, en el plazo de cinco días hábiles de recibida la solicitud o, en su caso, informar de las razones por las que estima no corresponde.
En el caso, el reclamo identificado con el No…, por su contenido, era una clara solicitud de rectificación de datos. No obstante, el responsable de la base de datos, BB, recién procedió a contestar por mail al denunciante con fecha 21 de junio (folio 72), sin perjuicio de lo cual, CC indicó que la efectiva rectificación se realizó el día 16 de junio (folio 69), ambas fechas vencido con exceso el plazo previsto en el artículo 15.

3. Potestad Sancionatoria.- Conforme lo prevé el artículo 35 de la LPDP, en redacción dada por el artículo 152 de la Ley No. 18.719, el Órgano de Control podrá aplicar a los responsables de bases de datos, encargados de tratamiento y demás sujetos alcanzados por el régimen de la Ley, en caso de que se violen sus disposiciones, las sanciones de observación, apercibimiento, multa, suspensión y clausura de la base de datos respectiva.
4. Satisfacción de la pretensión.- No obstante lo expuesto, no puede soslayarse que el propio denunciante emitió un comunicado vía correo electrónico al Órgano de Control, manifestando tener por satisfecha su pretensión. (situación que se asimila a la contenida en el artículo 86 del Decreto 500/99, que regula el desistimiento de la petición o renuncia al derecho)

-V-Conclusión

1. La situación denunciada, que en puridad implicó la violación de los artículos 7º y 22 de la LPDP por parte del BB., fue resuelta, aunque fuera del plazo legalmente previsto por el artículo 15 del mismo cuerpo normativo.

2. El denunciante, por su parte, dio por satisfecha su pretensión a través de comunicación expresa ante la URCDP.

3. En mérito a lo expuesto, a la calidad de primario del BB, a la entidad de la falta cometida y en atención a que ha dado cumplimiento al registro de sus bases de datos, se estiman dos caminos posibles, los que evaluará el Consejo Ejecutivo al momento de adoptar una decisión:

3.1. Imponer la sanción de observación por ser la más leve en la escala.

3.2. Archivar las actuaciones, sin perjuicio de instar al BB a que en adelante de cumplimiento al ejercicio de los derechos formulados por los titulares de los datos, en los plazos legalmente previstos.
Es todo cuanto tengo que informar.

Fdo. Dra. Ma. José Rodríguez
Derechos Ciudadanos

Informe N° 6212 de 6 de julio de 2011.

Se informa consulta de la Dirección Nacional de Medio Ambiente (DINAMA) acerca de la posibilidad de entregar datos de industria.

INFORME N°		EXPEDIENTE N°
6212	2011	2011-2-10-0000016

Montevideo, 6 de julio de 2011.
Ref. Consulta de la DINAMA.

-I-INTRODUCCIÓN

Con fecha 4 de febrero del corriente Marcelo Caffera denuncia ante la U.A.I.P. sobre la negativa por parte de la Dirección Nacional de Medio Ambiente (DINAMA) de entregar los informes que las plantas industriales sitas en Montevideo deben entregar cuatrimestralmente a DINAMA.
Asimismo solicita cantidad de inspecciones realizadas, multas aplicadas y muestras de efluentes por mes desde enero de 1999 al presente.

-II-ANTECEDENTES Y MARCO LEGAL

I) Previo a la presente denuncia, el interesado había realizado una denuncia contra la Intendencia de Montevideo (Expediente UAIP 2009/010) por la negativa a entregar los informes cuatrimestrales, que las empresas entregan a la Intendencia y DINAMA.

II) En el referido expediente, la URCDP se pronunció en el sentido de cuáles datos podían proporcionarse al solicitante y cuáles no, por considerarse datos personales de las empresas.
El Dictamen N° 9, de 28 de agosto de 2009 indica en su considerando 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 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)”.
En el mismo sentido, se pronuncia el Dictamen N° 2, de 21 de setiembre de 2009 de la UAIP.

III) Con fecha 6 de abril de 2011 DINAMA responde en el sentido que no existen inconvenientes a proporcionar la información sobre inspecciones realizadas, resultados de las muestras, fecha y monto de las multas, acciones intermedias tomadas entre inspecciones y multas, ubicación geográfica de las plantas industriales. Sin embargo no entregaría los datos referidos a: nombre de la empresa, cantidad producida de todos los productos, consumo de agua, consumo de energía, personal empleado por turno, días trabajados, caudales de los efluentes líquidos, detalle de las muestras.

IV) A fin de argumentar su posición, DINAMA cita una sentencia que suspende una resolución de acceso ya dictada, limitando la entrega de información, adjuntando la documentación del caso. Refiere a una acción de habeas data de varias empresas dedicadas al cultivo de maíz, contra un dictamen de AGESIC que indica que DINAMA debe exhibir la ubicación de los cultivos. El dictamen al que se hace referencia es de la UAIP, de fecha 22/4/11 y las empresas indican que no se contempló la opinión de la URCDP.
Con fecha 17/9/10 se dicta la Sentencia N° 55 del Juzgado Letrado de lo Contencioso Administrativo 4° que desestima la demanda.
En segunda instancia el Tribunal de Apelaciones en lo Civil de 4° turno (sentencia N° 273 de 22/11/10) hace lugar parcialmente a la demanda, limitando el acceso a los registros en que participan las sociedades accionantes.

V) La información solicitada refiere al impacto ambiental de ciertas prácticas industriales, por lo que puede considerarse un interés difuso, amparado en el art. 47 de la Constitución: "la protección del medio ambiente es de interés general."
El interés difuso deriva de la situación desprotegida que tiene la persona frente a las grandes empresas, refiere a derechos de la colectividad que van más allá de lo individual. Según la Dra. Leonie Garicoits: "El carácter de difuso emerge del hecho de la indeterminación de los límites de esa colectividad, que si bien posee una propiedad definitoria, desde el punto de vista cuantitativo resulta inconmensurable."22
Pero aun amparándose en el instituto de los intereses difusos, no es necesario asociar los datos obtenidos con el nombre de la empresa que presenta el informe.

VI) En el caso que no se pueda obtener el previo consentimiento de las empresas titulares para la entrega de los datos, los mismos se pueden disociar. Según el artículo 17 de la Ley N° 18.331: "Derechos referentes a la comunicación de datos.- Los datos personales objeto de tratamiento 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 debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo." Es por ello que se requiere el previo consentimiento informado de las empresas involucradas. El consentimiento, según el artículo 9° de la citada norma, debe ser: "libre, previo, expreso e informado, el que deberá documentarse." Si no existe el consentimiento, se procede a la disociación de datos.

VII) La disociación de datos se encuentra definida en el artículo 4° lit. G) de la Ley N° 18.331, como todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable.

22 -Garicoits, Leonie "Intereses difusos su protección legal y alcances" www.leoniegaricoits.com

La Agencia Vasca de Protección de Datos plantea técnicas de disociación en su Manual de Buenas Prácticas en Materia de Protección de Datos Personales. Según esta Agencia las técnicas de disociación deben destruir las referencias que permitan identificar al titular de los datos. Para eso se puede borrar o pintar el dato de forma que no se puede recuperar por ningún medio. Si no fuera posible la disociación entonces se debe asegurar la ilegibilidad de los datos mediante tachado.23

-III- CONCLUSIONES

La DINAMA está obligada a entregar la información solicitada siempre y cuando cuente con el consentimiento de los titulares en los términos del artículo 9° de la Ley N° 18.331.En caso de no contar con dicho consentimiento, se deberá proceder a la disociación de datos previo a la entrega.
En opinión de esta informante no tiene relevancia el hecho que exista una sentencia que revoque un previo pronunciamiento.

Fdo. Dra. Rosario Ierardo
Derechos Ciudadanos

23 - www.avpd.euskadi.net

Informe N° 6255 de 13 de julio de 2011.

Se informa denuncia sobre la idoneidad de acceder a información confidencial a través del ingreso de la cédula de identidad de las personas.

INFORME N°		EXPEDIENTE N°
6255	2011	2011-2-10-0000096

Montevideo, 13 de julio de 2011.

Ref. Denuncia de AA contra BB por incorporación del número de cédula de identidad del usuario para el acceso a su cuenta a través del Sitio Web del Organismo.

-I-Antecedentes

1. El Sr. AA formula denuncia ante la Unidad Reguladora y de Control de Datos Personales (URCDP) contra BB.

Sostiene que tan solo con ingresar el número de cédula de identidad del titular del servicio en el sitio Web de BB, se accede a su cuenta y directamente a información que en puridad es de carácter confidencial entre la empresa y el cliente, cuando según su opinión dicho acceso debería realizarse a través de un número de referencia que sea de exclusivo conocimiento entre las partes involucradas.

2. Se le otorga vista a BB, la que es evacuada en tiempo y forma.

Esta manifiesta que a raíz de la presente denuncia, a partir del 4 de mayo de 2011, quedó deshabilitada la posibilidad de acceder a la información del cliente por número de cédula de identidad, quedando solo disponible por referencia de cobro.

3. El 19 de mayo siguiente se le comunicó al denunciante que debía presentarse a tomar vista de las actuaciones, no habiendo comparecido hasta la fecha.

-II-Análisis

1. Competencia de la Unidad Reguladora y de Control de Datos Personales (URCDP).

El órgano de control tiene potestades para expedirse sobre la presente denuncia, en mérito a los cometidos atribuidos por el artículo 34 de la Ley Nº 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (en adelante LPDP).

2. Disposiciones aplicables al caso.

El sistema de consulta implementado por BB a través de su Sitio Web consiste en un tratamiento de datos en los términos establecidos por el artículo 4º literal M) de la LPDP, en tanto lo define como las “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”.

El mismo artículo, en su literal D) define dato personal como “información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables”.
El número de cédula de identidad en tanto puede determinar a una persona, es un dato personal.
Por su parte, el artículo 9° que prevé el principio del previo consentimiento informado, consagra que el tratamiento de datos personales será lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado. Añade dicha disposición que no será necesario dicho consentimiento cuando:

A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.

B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

E) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico.
Por su parte, el artículo 7º de la LPDP que regula el principio de veracidad de los datos, limita la recolección y el tratamiento de éstos a áquellos que revistan ciertas particularidades en relación con la finalidad para la cual hayan sido obtenidos. Esto es, que sean veraces, adecuados, ecuánimes y no excesivos.
Según el diccionario de la Real Academia Española, veraz refiere a la verdad; adecuado a lo apropiado a las condiciones, circunstancias u objeto de algo; ecuanimidad a imparcialidad de juicio; y excesivo, que excede y sale de la regla.

Si analizamos las acepciones en sentido global, extraemos que, en todo caso, los datos personales que sean objeto de tratamiento y se incorporen a una base de datos, deben ser realmente apropiados para la finalidad buscada. Deben mantener estricta conexión con el resto de los datos incorporados a la base de datos, pero además, y aunque resulten pertinentes por su naturaleza, debe ser absolutamente necesaria su inclusión en relación con la finalidad a la que se destina. 24

3. Acerca de la incorporación de la cédula de identidad al sistema de gestión y consulta.
Las disposiciones analizadas a la luz del sistema de consulta del Sitio Web de BB, indican que la incorporación del dato personal cédula de identidad del titular del servicio, para acceder a la información que el Organismo brinda al usuario, es inadecuada y excesiva.

24 REBOLLO, Lucrecio, SERRANO, Ma. Mercedes, “Introducción a la Protección de Datos”, 2a. Edición 2008, Madrid, pág. 144-145.

En efecto, cualquier persona que conozca el número de cédula de identidad de otra, podrá acceder fácilmente a la factura del consultado, tomando conocimiento de toda la información vinculada al titular del servicio, como nombre del cliente, dirección del suministro, facturas más recientes asociadas al suministro, información asociada de las últimas facturas emitidas y las refacturadas si las hubiera (fecha, consumo, potencia, importe, tipo, estado ref., fecha factura anulada).

4. Acerca de la solución adoptada por BB.
Sin perjuicio de lo expuesto, cabe destacar que BB, al tomar conocimiento de la presente denuncia por medio de la vista conferida, adoptó inmediatamente las medidas correctivas pertinentes, deshabilitando el acceso a la información del cliente por número de cédula de identidad y habilitándolo por número de referencia de cobro.
Esta modificación pudo ser corroborada, accediendo al Sitio Web de BB http://www.bb.com.uy/index.html tal como consta de la certificación notarial realizada por la Esc. Sandra Mazzone, que luce agregada al expediente electrónico.

Este extremo, sumado a la incomparecencia del denunciante, luego de haber operado la modificación que éste pretendía, amerita el archivo de las presentes actuaciones.

-III- Conclusiones

El número de cedula de identidad, en el caso planteado, se presenta como un dato excesivo para la finalidad buscada, cual es en todo caso que el usuario-cliente pueda acceder a toda la información relativa a su servicio contratado.

No obstante lo anterior y en mérito a que BB habiendo tomado conocimiento de la denuncia, adoptó medidas sustitutivas, habilitando el acceso del usuario mediante el número de referencia de cobro, dato que por ser de exclusivo conocimiento del titular del servicio se categoriza como pertinente y no excesivo con la finalidad buscada, corresponde el archivo de las presentes actuaciones.

Es todo cuanto tengo que informar.

Fdo. Dra. María José Rodríguez
Derechos Ciudadanos

Informe N° 6433 de 8 de agosto de 2011.
Se informa denuncia contra Central de Riesgos Crediticios.

INFORME N°		EXPEDIENTE N°
6433	2011	2011-2-10-0000336

Montevideo, 8 de agosto de 2011.
Ref. Denuncia. AA c/ BB, CC y DD.

Viene a conocimiento de la Unidad una denuncia de persona física, por figurar registrada en la base de datos personales de BB.
Dicho registro se produjo bajo la expresión “CC… CALIF:5 CASTIGADO POR ATRASO $ 15.814,90”, a consecuencia de una deuda de la madre de la denunciante (tarjeta de crédito del CC), cuando esta última poseía tarjeta adicional siendo menor de edad al momento de obtenerla.

Conferida la vista preceptiva a BB, los datos de la denunciante fueron finalmente eliminados de la base de datos según lo manifestara la denunciada, y según ha podido verificarlo también el suscrito informante al corroborar dicha eliminación mes a mes, desde agosto 2010 al mes en curso. Cada período consultado arroja la información “EL DOCUMENTO INGRESADO NO SE ENCUENTRA EN LA CENTRAL DE RIESGOS”.
La propia denunciante está en condición de realizar por sí misma la consulta respectiva, que no podrá arrojar otro resultado que el anotado.

Por todo lo expresado no es de recibo su ulterior queja de fs. 52, en la medida que los datos ya fueron eliminados con anterioridad como bien ratifica el denunciado en su postrer comparecencia del 29-07-2011.
Habiéndose cumplido lo ordenado por el Consejo, se hará saber a la denunciante que sus datos personales fueron eliminados de BB, procediéndose a informarle de dicha eliminación y clausurar estas actuaciones.

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 6447 de 9 de agosto de 2011.
Se informa denuncia relativa a robo de base de datos.

INFORME N°		EXPEDIENTE N°
6447	2011	2011-2-10-0000073

Montevideo, 9 de agosto de 2011.
Ref. Denuncia AA LTDA. C/ BB. Expediente remitido desde MEC-CPDC.

Se trata de una denuncia presentada originariamente ante la Comisión de Promoción y Defensa de la Competencia del Ministerio de Economía y Finanzas, en la que el citado organismo se declara incompetente y la remite a la URCDP por Resolución Nº 27/2011, dictada el 5 de abril de 2011.
De acuerdo al principio de especialidad que fija los márgenes de actuación de la URCDP (cf. Risso Ferrand, Derecho Constitucional t.III, p. 70 y ss., ed. Ingranusi, 1998) y habiendo escuchado a las interesadas (denunciante y denunciada), se sugerirá desechar la denuncia presentada al tiempo de sancionar a todos los involucrados por incumplimiento de la Ley Nº 18.331.

Como fundamento de lo primero (desechar la denuncia presentada), no se advierte que se haya prescindido del consentimiento de los titulares de los datos por parte de la competidora denunciada, a los efectos de las “solicitudes de afiliación”. Es lo que surge de la documentación aportada por la denunciante (fs. 6 a 8), donde los formularios respectivos lucen las firmas respectivas (facsímiles no desvirtuados por la denunciante). Por lo tanto, al figurar cumplido el “principio del consentimiento” (art. 9º de la Ley), la denuncia presentada carece de sustento. Todos los restantes hechos invocados o relacionados al caso, tanto por la denunciante como por la denunciada, resultan ajenos a la competencia de la Unidad.

En cuanto a lo segundo (sancionar a ambas partes por incumplimiento de la Ley Nº 18.331) se fundamenta en que, tanto la denunciada como la denunciante, realizan tratamientos de datos personales, y por ello les alcanzan las disposiciones de la Ley Nº 18.331 (arts. 2º, 3º primer inciso, 4º lits. K) y M) así como de su Decreto Reglamentario Nº 414/009, de 31 de agosto de 2009 (arts. 1º inc. 2, y 2º). No figurando inscriptas, ni en proceso de inscripción, sus bases de datos ante el Registro de bases de datos personales que lleva la URCDP, es manifiesto que incumplen con el “principio de legalidad” consagrado en el art. 6º de la Ley.
El descargo aportado por la socia de hecho de la denunciante en escrito presentado el 08-08-2011, no contiene elementos de juicio que desvirtúen el informe antedicho.

Se sugiere:
No hacer lugar a la denuncia presentada, y aplicar sanción a todos los involucrados-, por incumplimiento del principio de legalidad consagrado en el art. 6º de la Ley Nº 18.331, intimando a las empresas denunciante y denunciada a que registren sus bases de datos personales como ordena la norma legal.

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 6463 de 12 de agosto de 2011.
Se informa consulta de la Intendencia de Rivera sobre la posibilidad de publicar ciertos datos en sus servicios en línea.

INFORME N°		EXPEDIENTE N°
6463	2011	2011-2-10-0000448

Montevideo, 12 de agosto de 2011.
Ref. Consulta de la Intendencia de Rivera.

-I-INTRODUCCIÓN

Con fecha 5 de agosto del corriente la Intendencia de Rivera consulta a la URCDP sobre la posibilidad de publicar ciertos datos en los servicios de consulta de deuda e impresión de factura.

-II-CONSULTAS PLANTEADAS

I) Respecto a los tributos que se pueden publicar los servicios de deuda e impresión: contribución urbana, suburbana y rural; patente de rodados y permisos de circulación. Es facultad de las diversas intendencias el controlar el pago de los referidos tributos, por lo que el organismo podrá implementar este tipo de servicios a través de su página web según lo considere conveniente.

II) La pregunta siguiente refiere si se debe solicitar al usuario el número de padrón o el código interno del padrón para acceder a la información. Sobre tal punto, no corresponde a la URCDP pronunciamiento, siendo un tema de exclusiva competencia de la Intendencia.
Sobre el nivel de detalle a ser devuelto, se entiende que los campos: importe total de deuda vencida, importe total de cuotas a vencer, importe individual de cada una de las cuotas y detalle de los rubros que componen cada cuota, no revisten problema para su exhibición. Respecto al nombre del propietario, el mismo no debe ser exhibido. En el Dictamen N° 6, de fecha 11 de febrero de 2010, (referido a las cédulas catastrales) la URCDP indica en su considerando III): "Que de acuerdo con el principio de finalidad consignado en el artículo 8° de la LPDP, los datos personales no deben utilizarse para una finalidad distinta para la que fueron recabados, en el caso de marras, no sería necesario consignar el nombre de la persona para cumplir con la finalidad buscada ….."
En el mismo sentido, continúa el referido Dictamen recomendando la eliminación de los nombres de las cédulas expedidas por Catastro

III) Respecto a si se debe solicitar al usuario el número de padrón o el código interno del padrón para imprimir la correspondiente factura, no corresponde a la URCDP pronunciamiento, siendo un tema de exclusiva competencia de la Intendencia.

IV) Asimismo, tampoco es competente la URCDP a fin de pronunciarse si el usuario debe seleccionar parte de la deuda vencida, toda la deuda vencida o las cuotas a vencer a fin de generar la factura para impresión.

V) En virtud del artículo 8° de la citada Ley N° 18.331, no se deberían incluir en la factura web los datos

adicionales del padrón, nombre y RUC del propietario, nombre y RUC del contribuyente, dirección y teléfono del contribuyente y datos “información al contribuyente”; dado que no son necesarios para la finalidad consulta de deuda e impresión de factura.

VI) Finalmente, respecto a si la factura debe contener algún mensaje adicional, la Intendencia podrá incluir la cláusula de consentimiento para organismos públicos que se encuentra en nuestra página www.datospersonales.gub.uy en la pestaña Documentación/Destacados/Cláusulas.

-III-CONCLUSIONES

Se recomienda a la Intendencia de Rivera para los servicios de consulta de deuda e impresión de factura a través de su página web eliminar el dato nombre del propietario y no consignar los datos reseñados en el num. V del presente informe.
Se recomienda asimismo incluir la cláusula de consentimiento para organismos públicos.

Fdo. Dra. Rosario Ierardo
Derechos Ciudadanos

Informe N° 6518 de 22 de agosto de 2011.

Se informa consulta de la Intendencia de Montevideo sobre la posibilidad de publicar datos de las partidas que expide el Registro de Estado Civil.

INFORME N°		EXPEDIENTE N°
6518	2011	2011-2-10-0000484

Montevideo, 22 de agosto de 2011.
Ref. Consulta sobre adecuación de la publicidad de datos a la Ley Nro. 18331.

-I-La consulta

Se consulta sobre el proyecto de incluir en el sitio web institucional de la Intendencia Municipal de Montevideo, el índice del archivo que contiene los asientos básicos de las partidas que expide el Servicio de Registro de Estado Civil de dicha Intendencia.

La información aportada por el consultante, refiere a que dicha inclusión sería en calidad de "dato abierto", con acceso exclusivamente a: nombre completo de la persona; su fecha de nacimiento, matrimonio o defunción; año, sección y acta. No se incluiría la imagen de la partida asociada.
Se requiere la opinión de la Unidad, acerca de si la publicación de esta información en las referidas condiciones, vulnera el régimen de la Ley Nº 18.331, o bien resulta admisible teniendo en cuenta, además, la finalidad de facilitar el acceso de los interesados a las partidas registradas.

-II- Análisis y conclusiones

El derecho a la protección de los datos personales es un derecho fundamental reconocido por el art. 72 de la Constitución, y regulado por la Ley Nº 18.331, su modificativa Ley Nº 18.719, y sus decretos reglamentarios.
La URCDP puede "asistir y asesorar a las personas que lo requieran" y "emitir opinión toda vez que le sea requerida por las autoridades competentes" (art. 34 lits. A) y F) de la Ley Nº 18.331). La consulta presentada se acomoda a estas previsiones legales.
Uno de los principios generales del régimen es el "principio de consentimiento" del titular de los datos personales, aplicable a cualquier tratamiento que se desee realizar sobre datos personales (arts. 9º y 17 de la Ley). Por este principio, tanto la recolección (art. 9º de la Ley) como la comunicación a terceros de datos ya recolectados (art. 17 de la Ley), deben contar con el consentimiento libre, previo, expreso, informado y documentado de los titulares. Las excepciones a esta regla están previstas a texto expreso en estos mismos artículos de la Ley.

En respuesta al consultante se debe expresar que la publicación vía web con carácter abierto, de datos personales que exceden la excepción dispuesta por el art. 9º lit. C) de la Ley, no cumple con el régimen legal.

Tampoco cabe sostener la aplicación de otra clase de excepciones legales. El índice del archivo del Servicio no es una "fuente pública de información", y el tratamiento proyectado no encaja en "el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal"; tampoco existe "ley general" que habilite este tipo de comunicaciones (arts. 9º lits. A) y B), y 17 lit. A) de la Ley).

Por lo tanto el proyectado sistema previendo la inclusión de datos y hechos relevantes al estado civil de las personas como es el caso de los matrimonios y de las defunciones, y en definitiva cualquier otro tipo de dato personal que no sean aquéllos previstos por el art. 9º lit. C) de la Ley, vulnera el régimen jurídico de la protección de datos personales vigente en el país.

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 6549 de 26 de agosto de 2011.

Se informa denuncia por información publicada en un Diario de Sesiones del Parlamento.

INFORME N°		EXPEDIENTE N°
6549	2011	2011-2-10-0000334

Montevideo, 26 de agosto de 2011.
Ref. Denuncia al Parlamento Nacional.

-I-Antecedentes

Viene a conocimiento de la Unidad el planteo de la Dirección General de Comercio, Área Defensa del Consumidor, Ministerio de Economía y Finanzas (fs. 1 y 2) referente a varias denuncias practicadas por un particular, las que afectan a funcionarios del servicio primeramente nombrado, a uno en particular, y al propio organismo al que pertenecen, en nombre del cual actuaran aquéllos.

Las referidas denuncias dieron mérito a investigaciones administrativas internas en el organismo, al cabo de las cuales se ordenó su clausura por falta de mérito y pruebas. Mientras ello ocurría, las denuncias llegaron al Parlamento Nacional y fueron publicadas en forma extensa y textual en su sitio web.
Los afectados entienden que se debe eliminar la información publicada, y así lo solicitaron a la autoridad parlamentaria. Sin embargo ésta no tomó decisión al respecto, y se plantea que sea la Unidad la que resuelva el punto (fs. 2 y 193).

-II-Análisis

En primer lugar conviene hacer explícito el marco de competencia de la Unidad con relación al caso planteado.
La Unidad puede “asistir y asesorar a las personas que lo requieran” y “emitir opinión toda vez que le sea requerida por las autoridades competentes” (art. 34 lits. A) y F) de la Ley Nº 18.331). Ni una cosa ni la otra aparecen como hipótesis plausibles al caso, ya que los interesados no han hecho un planteo del rigor y precisión que las circunstancias daban mérito, si hubieran querido movilizar tales poderes de parte de la Unidad.

Véase lo ocurrido y sáquense las conclusiones pertinentes:
- la Dirección General de Comercio, Área Defensa del Consumidor, en definitiva la promotora de obrados, se limita a poner en conocimiento de la Unidad una serie cronológica de hechos, sin pedir nada en concreto (fs. 1);
- las funcionarias afectadas comparecen a posteriori, con la instrucción administrativa del caso prácticamente culminada, invocando intereses tanto propios como corporativos, y pidiendo que “se retire de la Web esta publicación...” (fs.197 y ss.) lo que claramente exorbita los poderes legales de la Unidad.

- el Prosecretario de la Cámara de Senadores, por su parte, actuando en nombre de la Presidencia de la Cámara de Senadores, se limita a expresar el 14 de junio de 2011, que la información objeto de disputa sigue publicada en el sitio web del Parlamento, y que "estaremos a lo que la Unidad competente en la materia resuelva" (fs. 193), omitiendo emitir pronunciamiento propio al respecto.
Se aprecia que desde el año 2004 ambos organismos han cruzado notas en relación al caso. La Dirección General de Comercio, Área Defensa del Consumidor ha insistido que se levante la información electrónica de marras, incluso lo ha peticionado al buscador GOOGLE que responde que eso debe ocurrir en el servidor del Parlamento, para que la información no aparezca más en las indexaciones de los motores de búsqueda de Internet. Si bien ninguno de estos petitorios han dado el resultado esperado por quienes lo promovieran, tampoco surge de autos una negativa expresa de los mismos, de parte de la autoridad parlamentaria.

Ciertamente en un caso como el ocurrente, son las propias partes las que tendrían que armonizar conceptos e intereses, en particular el órgano parlamentario que, hasta donde conoce la Unidad, no ha tomado una decisión expresa sobre el tema (negativa o positiva), y con ello favorece la insistencia del órgano del MEF.

Se trata de interlocutores estatales, por lo que aparece necesario, y casi que de orden, que se pongan de acuerdo en lo que cada uno debe hacer conforme a derecho. Y en punto a las personas físicas afectadas por estos hechos, en la medida que se sientan lesionadas en sus derechos o intereses, si no obtuvieran una solución oblicua satisfactoria como consecuencia de lo que resolvieran los organismos, siempre tienen a disposición las vías legales correspondientes para intentar la nulidad del acto y/o la reparación de los perjuicios sufridos.

El asunto planteado es una cuestión incardinada a los propios cometidos de órgano que recibió las denuncias y las publicó: si debió o no publicarlas, si procedía publicarlas pero en forma de versión pública (con datos personales anonimizados) y, finalmente, si procede eliminarlas o no y cuándo hacerlo en su caso. O sea que las opciones estuvieron y están al alcance de ser resueltas, por quienes deben resolverlas. Lo que no parece procedente, por la peculiaridad del asunto a examen y la forma en que se han procesado estas actuaciones, es que sea la Unidad la que se convierta en órgano dirimente de qué hacer y cómo hacerlo.

Por naturaleza y competencias, el Parlamento Nacional es la caja de resonancia mayor del país para recibir sugerencias, planteos, denuncias, etc. de parte de cualquier sujeto de derecho. Por tanto es cosa normal y ordinaria que reciba textos y documentos de la más diversa índole a tales propósitos.

No le corresponde a la Unidad pronunciarse sobre la pertinencia o no de publicar estos documentos o algunas especies de ellos en el sitio web parlamentario. En el Estado de Derecho esto no es posible, puesto que la URCDP es un órgano, si bien técnicamente autónomo, funcionando en la órbita del Poder Ejecutivo.

No le puede decir al Parlamento lo que debe hacer o dejar de hacer con las informaciones que recibe y procesa. Nada de esto puede o debe hacerlo la Unidad, so pena de ambientar un conflicto de poderes, o en el mejor de los casos exorbitar su propia competencia material (principio de especialidad). Se debe

tener presente que nadie le pidió a la Unidad un dictamen a propósito de ello, en los formales términos que habrían sido menester si esa hubiera sido la voluntad de los protagonistas del caso.

Al no haberse pedido que se emita una opinión ni que se asesore sobre el caso, no resulta aconsejable pronunciarse sobre el fondo del asunto. Son actitudes que no corresponde dejar entrever respuesta, frente a algo que no ha ocurrido.

-III-Conclusiones

1) Por la forma que se procesaron estas actuaciones, y la naturaleza especial del órgano que publicara la información cuyo borrado se pretende, no corresponde que la URCDP se pronuncie ni a favor ni en contra de dicho borrado.

2) La URCDP podrá, en cambio y si así se lo solicitara formalmente el órgano parlamentario, emitir opinión acerca de si procede o no el borrado peticionado en cumplimiento de la Ley Nº 18.331.

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 6684 de 15 de setiembre de 2011.

Se informa denuncia por envío de correo electrónico no deseado.

INFORME N°		EXPEDIENTE N°
6684	2011	2011-2-10-0000095

Montevideo, 15 de setiembre de 2011.
Ref. Denuncia contra BB.

La Ley Nº 18.331, de 18 de Agosto de 2008 con las modificaciones introducidas por la Ley Nº 18.719, de 27 de diciembre de 2010 (en adelante denominada LPDP)), y sus Decretos Reglamentarios Nros. 664/008, de 22 de diciembre de 2008 y 414/009, de 31 de Agosto de 2009 respectivamente, regulan el derecho fundamental de protección de datos personales, de las personas físicas y jurídicas.

El nombre de una casilla de correos electrónicos es un dato personal que ingresa en la definición amplia contenida en el art. 4º lt. D) de la LPDP.Su uso por terceros a fines publicitarios está permitido solamente en los casos que "...figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento" (art. 21 de la LPDP, redacción actual dada por el art. 152 de la Ley Nº 18.719).
Cuando no se dan estas hipótesis, ingresamos en lo que se conoce bajo el nombre de "spam". En el documento oficial español "Guía para la lucha contra el spam"25 se definen conceptos: "Actualmente se denomina Spam o "correo basura" a todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo se entiende por Spam cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico. Esta conducta es particularmente grave cuando se realiza en forma masiva."
Las explicaciones ofrecidas por la denunciada a fs 9 no satisfacen. Es claro que utiliza este mecanismo o vía publicitaria para promover su negocio. Pero no ha acreditado que lo haga dentro de los límites permitidos por el citado art. 21 de la LPDP, ante lo cual se concluye que ha existido infracción al régimen. Asimismo surge que la denunciada no ha inscripto sus bases de datos personales en la Unidad, contraviniendo por ello los arts. 28 y 29 de la LPDP.

La primariedad de los ilícitos cometidos hará que se aconseje la aplicación de la sanción mínima de "observación" (art. 35 de la LPDP en redacción actual dada por el art. 152 de la Ley Nº 18.719), e intimación a inscribir las bases de datos personales de que disponga la denunciada dentro del plazo de treinta días corridos, bajo apercibimiento de mayores sanciones.
Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

25 Agencia Española de Protección de Datos Personales. Consultable en https://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N-SPAM--ap-V.-30-mayo-cp-.pdf

Informe N° 6685 de 16 de setiembre de 2011.
Se informa consulta de la Junta Nacional de Drogas sobre el tratamiento de los datos de los usuarios.

INFORME N°		EXPEDIENTE N°
6685	2011	2011-2-10-0000584

Montevideo, 16 de setiembre de 2011.

-I- INTRODUCCIÓN

Con fecha 12 de setiembre del corriente la Junta Nacional de Drogas (JND) consulta a la URCDP sobre la gestión de los datos de usuarios.

-II- CONSULTA PLANTEADA

La JND, pide asesoramiento respecto a las potestades para gestionar la base de datos de los usuarios.
Según lo indicado, los datos que integrarían dicha base son: identificación de las personas en tratamiento y/o beneficiaras del sistema, ingreso, tratamiento, egreso y seguimiento posterior en los centros de atención especializada y gestión de servicios de inserción socio-laboral que ofrece la JND.
Dentro de los cometidos de la JND se encuentra: "la instrumentación de las directivas relacionadas con la fijación de la política nacional en materia de drogas, dirigida a la prevención del consumo problemático y tratamiento de la adicción a las drogas…"26, por lo que resulta lógico que dicho organismo sea responsable de la base de datos de usuarios de centros especializados en adicciones.

-III- MARCO LEGAL

Dicha base cuenta con datos especialmente protegidos, como son los datos de salud, que se encuentran reglamentados en los artículos 18 y 19 de la Ley N° 18.331. En el caso de datos de salud, para su tratamiento conforme a derecho deben respetarse los principios de secreto profesional, la normativa específica vigente y lo establecido en la presente Ley.

En el presente caso el tratamiento de datos se encuadra en la hipótesis del art. 18 inciso 2 "Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizados por ley…".
En lo que respecta a la Ley N° 18.331, la JND deberá respetar los principios de legalidad, veracidad, finalidad, seguridad, reserva y responsabilidad (arts. 5° a 12).

Respecto al previo consentimiento informado, no sería necesario en el presente caso, ya que opera la excepción del art. 17 lit. B), que remite al art. 9° B): "No será necesario el previo consentimiento informado

26 www.infodrogas.gub.uy

cuando (…) B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal…”
De todas maneras, y según lo dispuesto por el Decreto N° 414/009, la JND deberá inscribir la base de datos resultante en su calidad de responsable.

-IV-CONCLUSIONES

La JND deberá inscribir en carácter de responsable, la base de datos motivo de la consulta, atento a lo establecido por Decreto N° 414/009.
En el tratamiento de los datos especialmente protegidos, deberán tomarse en consideración los principios de legalidad, veracidad, finalidad, seguridad, reserva y responsabilidad de la Ley N° 18.331.

Fdo. Dra. Rosario Ierardo
Derechos Ciudadanos

Informe N° 6696 de 19 de setiembre de 2011.

Se informa consulta sobre comunicación de datos entre el Ministerio de Ganadería, Agricultura y Pesca y el Ministerio del Interior.

INFORME N°		EXPEDIENTE N°
6696	2011	2011-2-10-0000587

Montevideo, 19 de setiembre de 2011.
Ref. Consulta MGAP y MI.

-I-Antecedentes

La presente consulta refiere a la posibilidad de que el Ministerio de Ganadería, Agricultura y Pesca comunique datos al Ministerio del Interior en el marco de proyecto presentado como Fondo Concursable de AGESIC denominado “Fortalecimiento de la Seguridad del Movimiento de Semovientes”.
En el referido proyecto, el Ministerio de Ganadería, Agricultura y Pesca trasferiría los siguientes datos al Ministerio del Interior: número de DICOSE, número de caravana, número de padrón de campo, cédula de identidad del propietario (eventualmente puede requerirse también el nombre), identificación de la marca y razón social.

-II-Análisis

a. Aplicabilidad de la Ley N° 18.331.
Se está ante la presencia de datos personales conforme con la definición contenida en el artículo 4° literal d) de la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (en adelante LPDP) la que la define como aquella “información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables”.
En el caso de marras, estamos ante la presencia de datos personales, algunos determinados como el nombre, la cédula de identidad, el RUT, y otros determinables, por lo que es aplicable al caso concreto la LPDP.

b. Comunicación de datos
La consulta presentada refiere a una comunicación de datos entre el Ministerio de Ganadería, Agricultura y Pesca y el Ministerio del Interior. La comunicación de datos está definida en el artículo 4° literal b) de la LPDP en los siguientes términos “toda revelación de datos realizada a una persona distinta del titular de los datos”.
Según el artículo 17 de la LPDP, los datos personales objeto de tratamiento 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 debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.

Asimismo, el artículo 17 prevé en forma taxativa los casos en los cuales no es necesario recabar el consentimiento del interesado. En el caso de marras sería aplicable la excepción relativa a que no es necesario recabar el consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, la cual es aplicable por la remisión que hace el literal B) del artículo 17 de la LPDP.
Esta excepción reconoce su fuente en España, en la Ley 15/1999, y a su respecto se ha dicho que "el tratamiento de los datos personales no precisará del consentimiento de los afectados cuando sea preciso para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias". (Protección de Datos Personales para Administraciones Locales, APCM, pág. 151).

El Ministerio de Ganadería, Agricultura y Pesca brindará la información que surge de su Sistema Nacional de Información Ganadera. El Sistema Nacional de Información Ganadera (SNIG) es un sistema de información que tiene como objetivo principal asegurar la trazabilidad del ganado vacuno desde el establecimiento de origen del animal hasta el frigorífico, tanto individualmente como por grupos de animales, de acuerdo con las disposiciones y reglamentaciones del MGAP (Fuente: http://www.snig.gub.uy/portal/hgxpp001.aspx?2,1,59,O,S,0,MNU;E;28;1;16;2;MNU;).

El Ministerio del Interior, organismo receptor de la información, solicita la información dentro de las funciones propias del organismo (artículo 9° literal B) de la LPDP). En el caso de marras, el Ministerio de Interior tiene como cometido asegurar la seguridad nacional y para ello debe prevenir y combatir el delito. Dentro de los delitos que se deben prevenir y reprimir se encuentra el abigeato. La Ley N° 17.826, de 14 de setiembre de 2004, en su artículo 1° sustituye el artículo 258 del Código Rural regulando el delito en los siguientes términos:

> "ARTÍCULO 258.- Comete el delito de abigeato y será castigado con tres meses de prisión a seis años de penitenciaría, el que fuera de las ciudades o pueblos, con intención de matar, diere muerte, faenare o se apoderare con sustracción de ganado vacuno y bubalino, caballar, lanar, cabrío, porcino, cualquier otra especie de corral o criadero, colmenas, cueros, lanas, pieles, plumas o cerdas ajenos, y el que marcare o señalare, borrare o modificare las marcas y señales de animales o cueros ajenos, para aprovecharse de ellos.

La pena de prisión podrá sustituirse con horas de trabajo en servicio a la comunidad. El Juez de la causa y determinará la clase de servicio a cumplirse, el lugar y la cantidad de horas, así como el contralor del cumplimiento de dicha sanción".

Por su parte, el artículo 2° de la Ley Orgánica Policial indica que, como policía administrativa, le corresponde el mantenimiento del orden público y la prevención de los delitos.

Por tanto, en la presente consulta se verifica la excepción contenida en el artículo 9° literal B) de la Ley, por lo que la comunicación de datos es legítima ya que el Ministerio de Interior está ejerciendo funciones propias del organismo y los datos provienen de otro organismo, por lo que no sería necesario recabar el

consentimiento de los titulares.

Complementariamente, corresponde decir que no se considerarán aplicables ninguna de las otras excepciones contenidas en el art. 9º de la LPDP.

c. Otros aspectos de interés

Igualmente se hace aplicable el resto de la normativa vigente, sobre todo los principios que regulan la protección de datos.

En este sentido, es aplicable el principio de veracidad de los datos, el cual establece que los datos deben ser adecuados y no excesivos en relación con la finalidad para la cual se hubieren obtenido.

Asimismo, resulta aplicable el principio de seguridad de los datos por el cual los responsables de las bases de datos deben adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales.

-III-Conclusiones

Estamos ante una consulta que involucra datos personales por lo que es aplicable la Ley N° 18.331, de 11 de agosto de 2008.

Se trata de una comunicación de datos entre el Ministerio de Ganadería, Agricultura y Pesca y el Ministerio de Interior a efectos de prevenir y reprimir el delito de abigeato.

El Ministerio de Interior es el organismo competente en lo que respecta a la prevención y represión del delito de abigeato y el Ministerio de Ganadería, Agricultura y Pesca lleva un sistema nacional de información ganadera donde se encuentra la información necesaria para llevar a cabo su función.

La Ley prevé que para comunicar datos es necesario contar con el consentimiento del titular, siendo las excepciones taxativas.Una de las excepciones previstas, donde no es necesario el consentimiento, es que se trate de organismos en el ejercicio propio de sus funciones. En la situación de marras no es necesario recabar el consentimiento porque se verifica la mencionada excepción y, por tanto, no habría infracción a la LPDP.

Por último, se recomienda tener en cuenta el resto de las previsiones contenidas en la LPDP.

Fdo. Dra. Flavia Baladán

Derechos Ciudadanos

Informe N° 6720 de 20 de setiembre de 2011.
Se informa consulta sobre transferencia internacional de datos.

INFORME N°		EXPEDIENTE N°
6720	2011	2011-2-10-0000594

Montevideo, 20 de setiembre de 2011.
Ref. Consulta Royal & Sunalliance Seguros S.A..

-I-Antecedentes

La presente consulta alude a una encuesta a realizarse a los corredores de Latinoamérica de Royal & Sunalliance Seguros SA (RSA) a través de un proveedor externo. El contacto con los corredores se realizará desde Argentina.
Se aclara que RSA, sucursal de Londres, firmó un contrato con el proveedor para toda la región. No obstante ello, se está formalizando un contrato en Argentina.

Además, se indica que los datos a comunicar son los nombres, teléfonos y dirección de correo electrónico de los corredores incluidos en la base de datos "RSA-UY Corredores", la que se encuentra en proceso de inscripción ante la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP).
En la consulta, se solicita se informe si es necesario presentar información adicional, cuál y de qué forma.

-II-Análisis

a. Aplicabilidad de la Ley N° 18.331
En virtud de tratarse de información de una base de datos que se encuentra en el país, la cual contiene datos personales, es aplicable la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (en adelante LPDP).

La definición de base de datos está contenida en el artículo 4° de la LPDP en los siguientes términos "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".

b. Transferencia internacional de datos
La consulta se refiere a la posibilidad de realizar una transferencia internacional de datos, por la cual se enviará información de la base de datos de corredores de Uruguay a un proveedor contratado por RSA en Argentina.
A su vez, se informa que RSA, con sucursal en Argentina, a pesar del acuerdo marco existente, está haciendo un contrato propio, del cual no se informan las condiciones ni los motivos por los cuales se está realizando dicho contrato.

Según lo dispuesto en el artículo 4° literal H) del Decreto N° 414/009, se considera transferencia internacional de datos aquel tratamiento 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.

La LPDP, en su artículo 23, prohíbe la transferencia de datos personales de cualquier tipo 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.

Asimismo, el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, mediante Resolución N° 17, de 12 de junio de 2009, indicó que se consideran apropiados para la transferencia internacional de datos aquellos países que cuenten con normas de protección de datos adecuados y medios para asegurar su aplicación eficaz. Y agrega que entre ellos, se encuentran comprendidos los países que la Comisión Europea considera que garantizan las condiciones indicadas.

Por lo que el principio es que si la transferencia de datos se realiza a países adecuados no regiría la referida prohibición.
Según lo informado por la consultante, los datos se transferirán a Argentina desde donde se prestará el servicio. Dicho país, conforme con la Decisión 2003/490/CE, de la Comisión de 30 de junio de 2003, es considerada país adecuado.
Por tanto, no habría problema con el tratamiento de datos en ese país ya que es un país adecuado para realizar transferencias internacionales de datos.

c. Inscripción de la base de datos
La base de datos fue presentada con fecha 8 de setiembre de 2010, estando el trámite aún en proceso de inscripción.Por tanto, corresponde informar que se realizará transferencia internacional de datos, a qué países, con qué finalidad, y cuáles datos.

d. Otros aspectos de interés
En relación con el tipo de datos a transferir, nombre, teléfono y dirección de correo electrónico, se consideran que son los adecuados para la finalidad para la cual se están requiriendo, con lo que se verifica el cumplimiento del principio de veracidad de los datos regulado en la LPDP.Igualmente, resulta de aplicación al tratamiento de datos personales toda la normativa de protección de datos, sobre todos los principios que la regulan.Por lo que, en el caso concreto, se deberá dar cumplimiento con el resto de los derechos y obligaciones que instaura la LPDP.

-III-Conclusiones

La consulta refiere a una transferencia de datos personales a Argentina donde se va a realizar una encuesta a los corredores de RSA.
La información que se va a transferir proviene de la base de datos “RSA-UY Corredores” y es relativa a los nombres, teléfonos y direcciones de correo electrónicos.

Según la Ley, la transferencia internacional de datos está prohibida a países que no sean adecuados.
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, considera que se pueden transferir datos a aquellos países que cuenten con un nivel adecuado de protección.

Argentina, conforme con la Decisión 2003/490/CE, de la Comisión de 30 de junio de 2003, es considerado un país adecuado.
En virtud de ello, la transferencia internacional de datos a Argentina estaría permitida.
Con respecto a la información que la empresa debe brindar, se informa que deberá informar con respecto a la base de datos objeto de consulta, que se va a realizar una transferencia internacional de datos, el destino de los datos, qué datos se van a comunicar y con qué finalidad.

Por último, se debe tener presente que se debe dar cumplimiento al todo el resto de la normativa que regula la protección de datos.

Fdo. Dra. Flavia Baladán
Derechos Ciudadanos

Informe N° 6744 de 23 de setiembre de 2011.

Se informa consulta de Obras Sanitarias del Estado (OSE) sobre tratamiento de los datos de salud de los funcionarios.

INFORME N°		EXPEDIENTE N°
6744	2011	2011-2-10-0000603

Montevideo, 23 de setiembre de 2011.

-I-INTRODUCCIÓN

Con fecha 22 de setiembre del corriente, OSE consulta a la URCDP sobre la gestión de los datos de salud de sus funcionarios.

-II-CONSULTA PLANTEADA

Según lo indicado, Servicios Médicos de OSE consulta si puede tratar y recolectar los datos de salud de los funcionarios, con su consentimiento. Asimismo, si por la función certificadora constituye una excepción a la solicitud de consentimiento y a la prohibición de recolectar y tratar datos de salud.

Dicha base cuenta con datos especialmente protegidos, como son los datos de salud, que se encuentran reglamentados en los artículos 18 y 19 de la Ley N° 18.331. En el caso de datos de salud, para su tratamiento conforme a derecho deben respetarse los principios de secreto profesional, la normativa específica vigente y lo establecido en la Ley N° 18.331.

La Ley orgánica de OSE N° 11.907, en su artículo 19 lit. b) establece como requisito para el ingreso de trabajadores “aptitud física y moral demostrada, respectivamente por el Carné de Salud….” En ese sentido, la Ley faculta a OSE a establecer los mecanismos para certificar a los trabajadores en caso de enfermedad. Entonces, para el caso concreto, la recolección y tratamiento encuadra en la hipótesis del art. 18 inciso 2° “Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizados por ley…”.

Respecto al previo consentimiento informado, se entiende que no sería necesario en el presente caso, ya que opera la excepción del art. 17 lit. B) de la Ley N° 18.331, que remite al art. 9° B): “No será necesario el previo consentimiento informado cuando (…) B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal…”

La siguiente consulta refiere a la posibilidad de ceder los datos a distintas unidades dentro del organismo. Como ejemplos, menciona a la Sección Sumarios y la Comisión de Seguridad y Salud Laboral de OSE. En el caso de la Comisión contempla comunicaciones a terceros.

En el caso de comunicación de datos dentro del mismo organismo, no puede ser considerada cesión.
En el caso de ceder datos a terceros, se debe contar con el consentimiento del titular, o realizar la disociación de los titulares, de acuerdo con lo establecido por el lit. c) del artículo 17 de la Ley N° 18.331. Las formas de recabar el consentimiento, se encuentran reguladas en el art. 6° del Decreto Reglamentario N° 414/2009.

La última consulta refiere a si el Servicio Médico de OSE puede tener una base de datos de salud. En este punto cabe precisar que el art. 19 de la Ley permite a los profesionales vinculados a las ciencias de la salud, pueden recolectar este tipo de datos, respetando los principios de secreto profesional, la normativa específica vigente y lo establecido en la Ley N° 18.331.
Esta base de datos debe ser inscripta, de acuerdo con lo establecido por el Decreto Reglamentario N° 414/2009.

-III-CONCLUSIONES

El Servicio Médico de OSE puede recolectar y tratar datos de salud de los trabajadores de OSE, para el cumplimiento de sus funciones.
Para ceder datos de salud fuera del OSE, deberá recabar el consentimiento de los titulares, o disociar los datos.
En el tratamiento de los datos especialmente protegidos, deberán tomarse en consideración los principios de legalidad, veracidad, finalidad, seguridad, reserva y responsabilidad de la Ley N° 18.331.
OSE deberá inscribir en carácter de responsable, la base de datos motivo de la consulta, atento a lo establecido por Decreto N° 414/009.

Fdo. Dra. Rosario Ierardo
Derechos Ciudadanos

Informe N° 6820 de 11 de octubre de 2011.

Se informa consulta del Ministerio de Trabajo y Seguridad Social relativa a la transmisión de las planillas de trabajo a la Dirección Nacional de Bomberos.

INFORME N°		EXPEDIENTE N°
6820	2011	2011-2-10-0000646

Montevideo, 11 de octubre de 2011.
Ref. Consulta de MTSS sobre entrega de Planillas de Trabajo a Bomberos.

-I-Introducción.

El Ministerio de Trabajo y Seguridad Social formula consulta a la Unidad Reguladora y de Control de Datos Personales (URCDP), en virtud de solicitar opinión en el caso de la realización de una comunicación de las planillas de trabajo llevadas por aquél, a la Dirección Nacional de Bomberos con el objetivo de controlar que las empresas que cuentan con habilitación de Bomberos mantengan personal capacitado en el marco de los cursos de capacitación externa que brinda dicha Institución.
Dicha consulta, involucra aspectos relacionados con la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales en virtud de que las Planillas de Trabajo que las empresas deben presentar ante el Ministerio, contienen datos personales de los empleados y de las empresas.
En virtud de la consulta recibida y en cumplimiento de las facultades que le son otorgadas en el artículo 34 de la Ley, la Unidad procede a la sustanciación de ésta.

-II-Análisis

II.a. Marco Normativo.

A efectos del encuadre de la presente consulta, resulta pertinente referir a las disposiciones legales y reglamentarias que tienen relación directa con el tema.
En primer lugar, debemos analizar la normativa que regula los denominados documentos de control de trabajo establecida por el Decreto Nº 108/007, de 22 de marzo de 2007.
En cuanto a las planillas de control de trabajo determina que deben ser llevadas por todas las empresas, sean personas físicas o jurídicas, de cualquier naturaleza, incluso las personas públicas no estatales, que posean personal dependiente.

Los aspectos más relevantes de estas disposiciones para nuestra materia son las que establecen cuál debe ser el contenido de las planillas de control de trabajo.
El Decreto dispone en su artículo 9º que en las planillas debe constar respecto a la empresa la razón social, naturaleza jurídica, domicilio y actividad, grupo y subgrupo salarial, número de RUT, número de BPS o caja paraestatal que corresponda, y fecha de inicio de actividades. En caso de ser una sociedad comercial debe contener además de lo anterior el nombre de un director, administrador o gerente y su cédula de identidad.

Respecto a los trabajadores debe constar nombre, fecha de nacimiento, sexo categoría laboral, fecha de ingreso y egreso si la hubiera, salarios en moneda nacional, horarios de trabajo y descansos intermedios y semanales. Por otra parte, la planilla tiene un espacio de Observaciones donde es posible anotar todo otro dato de interés para la relación laboral.

Por otra parte, debemos analizar la normativa que establece la obligatoriedad de que las empresas cuenten con determinada cantidad de personal instruido en materia de defensa contra siniestros.
La Ley Nº 15.896, de 15 de setiembre de 1987, en su artículo 7º, dispone que todo establecimiento comercial o industrial obligatoriamente debe mantener instruido en el manejo y utilización de los elementos de defensa contra siniestros, a un número adecuado de su personal según lo disponga la reglamentación.

El Decreto 547/009, de 7 de diciembre de 2009 dispone que la capacitación e instrucción de los dependientes estará a cargo exclusivamente de la Dirección Nacional de Bomberos, y será de cargo del titular del establecimiento pagar el precio por ello. Se dispone además la creación de un reglamento interno que se someterá a aprobación del Ministerio del Interior. Dicho reglamento fue aprobado por Resolución del Ministerio del Interior de fecha 24 de marzo de 2011.
Del análisis de la normativa vigente en la materia surgen para las empresas las obligaciones de presentar las planillas de trabajo así como de mantener personal capacitado en materia de siniestros por la Dirección Nacional de Bomberos.

II.b. Análisis desde la normativa de protección de datos personales.
De acuerdo a la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP) consagra en su artículo 17º los derechos referentes a la comunicación de datos. Establece como principio que los datos pueden ser comunicados con el previo consentimiento del titular de éstos y para el cumplimiento de los fines relacionados directamente con el interés legítimo de su titular. El artículo establece además los casos, en forma taxativa, en que no será necesario el consentimiento del titular de los datos para su comunicación. Entre las hipótesis previstas se encuentran los supuestos determinados por el artículo 9º de la Ley.
El mencionado artículo prevé las hipótesis en las cuales no se requiere consentimiento del titular de los datos para el tratamiento de éstos.
En el caso planteado en la consulta debemos analizar la hipótesis prevista por el artículo 9º literal B) de la Ley. Dicha disposición excepciona de consentimiento del titular en el caso de que los datos “se recaben para el ejercicio de las funciones propias de los poderes del Estado o en virtud de una obligación legal”.
De acuerdo a la normativa mencionada, la Dirección Nacional de Bomberos solicita al Ministerio de Trabajo las planillas de trabajo presentadas por las empresas con el objetivo de controlar que éstas cumplan con la obligación legal que establece la Ley Nº 15.896.
La Dirección Nacional de Bomberos solicita los datos en virtud del cumplimiento de cometidos específicos que le son asignados por la Ley. Por ello, podríamos concluir que dichos datos se recaban en el marco del ejercicio de sus funciones propias.
Por tanto, en la presente consulta se verifica la configuración de la excepción prevista en el artículo 9° literal B) de la Ley, por lo que la comunicación de datos es legítima. Ello en virtud de que la Dirección Nacional

de Bomberos está ejerciendo funciones propias del organismo.
Por otra parte, y en forma complementaria Se podría aplicar en forma parcial la excepción dispuesta en el artículo 9º literal C) respecto a los datos contenidos en las planillas de trabajo, únicamente respecto a los datos mencionados taxativamente por la Ley.

-III-Conclusiones.

Partimos de la base de que en la consulta planteada, resultan aplicables las disposiciones en materia de Protección de Datos Personales reguladas por la Ley Nº 18.331, de 17 de octubre de 2008.
Dentro de sus disposiciones la Ley prevé que para comunicar datos es necesario contar con el consentimiento del titular. Establece además un elenco de excepciones en forma taxativa.
La Dirección Nacional de Bomberos es un organismo público que en ejercicio de sus funciones, solicita los datos al Ministerio de Trabajo y Seguridad Social, que es quien puede brindarle la información sobre cuántos empleados tienen las empresas y cuándo ingresan y egresan de éstas, con el objetivo de controlar la obligación de capacitar al personal en materia de siniestros, que tienen las empresas.
De acuerdo a ello, el caso podría incluirse en la hipótesis prevista en el artículo 9º literal B) de la Ley, donde se indica que no es necesario el consentimiento del titular, cuando se trate de organismos en el ejercicio propio de sus funciones.
Por último, se recomienda tener en cuenta todos los principios contenidos en la LPDP.

Fdo. Dra. Jimena Hernández
Derechos Ciudadanos

Informe N° 6845 de 19 de octubre de 2011.
Se informa consulta del Hospital de Clínicas relativa a comunicación de datos al Fondo Nacional de Recursos.

INFORME N°		EXPEDIENTE N°
6845	2011	2011-2-10-0000678

Montevideo, 19 de octubre de 2011
Ref. Consulta sobre datos personales realizada por el Hospital de Clínicas.

-I-Antecedentes

Se presenta consulta realizada por la Dra. Mariela Vega, en representación del Hospital de Clínicas de la Universidad de la República, a la Unidad Reguladora y de Control de Datos Personales (URCDP).
La consulta refiere a la posibilidad de que el Hospital de Clínicas comunique datos de los pacientes que reciben tratamiento por tabaco, al Fondo Nacional de Recursos a efectos de que este último brinde la medicación necesaria.
En ese marco se adjunta nota con los datos solicitados. En ella se requieren los siguientes datos: nombres y apellidos, domicilio, teléfono, fecha de nacimiento, institución en la que se asiste, la medicación indicada, fecha en que dejó de fumar, si tuvo accidentes cardiovasculares, hipertensión descontrolada, arritmia con riesgo vital, diabetes descontrolada, y en el caso de que sea de sexo femenino, si está embarazada o en período de lactancia.

Por otra parte, se informa que el Fondo Nacional de Recursos creará una base de datos que podrá ser accedida por el Hospital de Clínicas. También se informa que el Fondo Nacional de Recursos disociará la información a efectos de confeccionar información estadística.
El objetivo de la consulta es determinar la necesidad de recabar el previo consentimiento informado del paciente para que brinde sus datos personales, y si son adecuados los datos solicitados. Se consulta, asimismo, respecto a la finalidad para la cual deberían otorgarlo (recolección, tratamiento, etc.).

-II-Análisis

Aplicabilidad de la Ley N° 18.331.
En la consulta se tratan datos personales conforme con la definición contenida en el artículo 4° literal d) de la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (en adelante LPDP) la que los define como aquella “información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables”.

En el caso de marras, estamos ante la presencia de datos personales tales como los nombres y apellidos, domicilio, fecha de nacimiento, entre otros, lo que hace aplicable al caso concreto la LPDP.
Comunicación de datos
La presente consulta refiere a una comunicación de datos que realiza el Hospital de Clínicas respecto de

los pacientes a los cuales se prescribe medicación para curar el tabaquismo. La medicación es brindada por el Fondo Nacional de Recursos, el cual para poder realizarlo, necesita recabar determinados datos personales de los pacientes. Surge del expediente que es intención del Hospital de Clínicas recabar el consentimiento informado de los titulares para informarles que sus datos serán comunicados al Fondo Nacional de Recursos a efectos de que se efectivice el tratamiento.

En virtud de ello, es necesario estudiar la legalidad de la situación a la luz de la normativa vigente.
En primer lugar, se debe tener presente que el artículo 4° literal b) de la LPDP define la comunicación de datos en los siguientes términos: "toda revelación de datos realizada a una persona distinta del titular de los datos".

En segundo lugar, según el artículo 17 de la misma norma, los datos personales objeto de tratamiento 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 debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.
En la consulta realizada se expresa que se recabará el consentimiento informado de los titulares por lo que se está dando cumplimiento a los requisitos solicitados por la norma.

Es de interés tener presente que el Hospital de Clínicas de la Universidad de la República tiene como misión "Brindar atención a la salud de las personas, de calidad, con profundo respeto y compromiso hacia ellas; a través de la cual, el Hospital deviene ámbito formador de recursos humanos y de generación de conocimientos, contribuyendo al desarrollo del nivel de salud de la población, optimizando la utilización de los recursos que a tales fines le son confiados".27 Siendo su principal función ser un hospital general, de adultos y para episodios con breve período de estadía, de alta complejidad y de referencia nacional en lo que competa.28

Por su parte, el Fondo Nacional de Recursos fue creado por la Ley N° 16.343, de 24 de diciembre de 1992. Su misión consiste en brindar cobertura financiera a procedimientos de medicina altamente especializada para toda la población, sin distinciones.29 Dentro de sus funciones se encuentra brindar determinados medicamentos que no puede cubrir el propio paciente.

Por tanto, podemos decir que ambas instituciones estarían realizando la comunicación de datos dentro del marco de sus competencias. En consecuencia, en el caso de marras la comunicación de datos se considera legítima, verificándose todos los requisitos necesarios para su realización.

27 http://www.hc.edu.uy/index.php?option=com_content&task=view&id=19&Itemid=60

28 http://www.hc.edu.uy/index.php?option=com_content&task=view&id=19&Itemid=60

29 http://www.fnr.gub.uy/institucional-0

También en la consulta se requiere que se determine el alcance del consentimiento. Si se debe recabar respecto a la recolección y/o al tratamiento de los datos personales. En este sentido, esta informante entiende que se debe informar al paciente la finalidad para la cual se le están solicitando los datos (esto es, comunicarlos al Fondo Nacional de Recursos para acceder a determinada medicación) y éste debe brindar su consentimiento en forma libre y expresa.

En cuanto al tipo de datos solicitados indicados en los antecedentes de este informe corresponde informar que se consideran adecuados, en tanto se trata de datos identificatorios del paciente así como los datos necesarios para su correcta modificación.
Ahora bien, el artículo 17 de la LPDP también prevé en forma taxativa los casos en los cuales no es necesario recabar el consentimiento del interesado.

En el caso de marras, sería aplicable la excepción relativa a que no es necesario recabar el consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, la cual es aplicable por la remisión que hace el literal B) del artículo 17 de la LPDP. Esta excepción reconoce su fuente en España, en la Ley 15/1999, y a su respecto se ha dicho que "el tratamiento de los datos personales no precisará del consentimiento de los afectados cuando sea preciso para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias".30 Corresponde analizar si es aplicable esta excepción a este caso concreto.

Además de las competencias de las Entidades involucradas referidas anteriormente, corresponde hacer referencia a la aplicabilidad de la Ley N° 17.793, de 16 de julio de 2004, que aprueba el Convenio Marco de la Organización Mundial de la Salud. Dicho Convenio tiene como objetivo proteger la salud humana, brindando un marco para las medidas contra el control de tabaco que deberán adoptarse a nivel nacional, regional e internacional. Es de destacar que el artículo 14 literal c) de la referida norma establece que cada Estado Parte deberá establecer en los centros de salud y de rehabilitación programas de diagnóstico, asesoramiento, prevención y tratamiento de la dependencia del tabaco.

En virtud de que el Convenio es aplicable en nuestro país. Que el Hospital de Clínicas es una Entidad que brinda asistencia a los pacientes, en el caso concreto posee una policlínica para el tratamiento del tabaquismo. Y que el Fondo Nacional de Recursos brinda los medicamentos necesarios para el tratamiento de dicha enfermedad se puede considerar aplicable al caso concreto la excepción contenida en el literal c) del artículo 17 de la Ley, no siendo necesario recabar el previo consentimiento de los titulares de los datos. Complementariamente, corresponde decir que no se considerarán aplicables ninguna de las otras excepciones contenidas en el art. 9º de la LPDP.
Otros aspectos de interés
Con respecto al acceso a la base de datos que llevaría el Fondo Nacional de Recursos, se considera correcto y necesario el acceso por parte de personal que deberá estar debidamente autorizado de forma tal

30 Protección de Datos Personales para Administraciones Locales, APCM, pág. 151

que se dé cumplimiento al principio de seguridad de los datos. Esto es, a efectos de preservar la seguridad, integridad y confidencialidad de los datos.
También se considera correcto que cuando el Fondo Nacional de Recursos considere adecuado realizar estadísticas relativas a los efectos de los tratamientos realizados disocie los datos personales. En ese procedimiento se recomienda se tenga presente que desde la perspectiva de la protección de datos disociar los datos es "todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable" (artículo 4° literal g) de la LPDP).
Igualmente se hace aplicable al caso concreto el resto de la normativa vigente, sobre todo los principios que regulan la protección de datos.

En este sentido, es aplicable el principio de veracidad de los datos, el cual establece que los datos deben ser adecuados y no excesivos en relación con la finalidad para la cual se hubieren obtenido.
Asimismo, resulta aplicable el principio de seguridad de los datos por el cual los responsables de las bases de datos deben adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales.

-III-Conclusiones

La presente consulta refiere a una comunicación de datos del Hospital de Clínicas al Fondo Nacional de Recursos.
Dicha comunicación de datos se realiza en virtud de que el Fondo Nacional de Recursos provee los medicamentos necesarios para el tratamiento de la enfermedad a aquellas personas que por razones económicas no pueden adquirirlos.El Hospital de Clínicas informa que recabará el consentimiento de los titulares para comunicar estos datos. Se considera adecuada la forma que se recabará el consentimiento, la información solicitada y se recomienda que se informe para qué serán tratados los datos.
Asimismo, conforme con las competencias asignadas a cada Entidad y en virtud de lo dispuesto por la Ley N° 17.793, de 16 de julio de 2004, sería posible comunicar datos sin recabar el consentimiento de los titulares ya que se configuraría la excepción contenida en el literal c) del artículo 17 de la Ley. Esto es, Entidades Públicas en ejercicio propio de sus funciones.
Por último, se recomienda tener presente las consideraciones realizadas en el literal c) del presente informe.
Es todo cuanto tengo que informar.

Fdo. Dra. Flavia Baladán
Derechos Ciudadanos

Informe N° 6854 de 18 de octubre de 2011.

Se informa consulta del Ministerio de Trabajo y Seguridad Social relativa a la comunicación de datos contenidos en las planillas de trabajo al Ministerio de Transporte y Obras Públicas.

INFORME N°		EXPEDIENTE N°
6854	2011	2011-2-10-0000687

Montevideo, 18 de octubre de 2010.
Ref. Consulta de MTOP sobre entrega de nóminas de empleados registradas en Planillas de Trabajo de MTSS.

-I-Introducción.

El Ministerio de Transporte y Obras Públicas formula consulta a la Unidad Reguladora y de Control de Datos Personales (URCDP), sobre la solicitud de datos que realizara al Ministerio de Trabajo y Seguridad Social relativa a una comunicación de datos contenidos en las planillas de trabajo llevadas por éste.

La finalidad de la mencionada solicitud radica en el diseño por parte del MTOP de un Sistema de Información de Transporte de Carga Terrestre y guías de carga. Para el ingreso en las guías es necesario verificar que los profesionales registrados o que estén enviando información pertenezcan a la empresa correspondiente. Para ello requieren la información contenida en las planillas de trabajo.

La consulta presentada involucra aspectos relacionados con la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales, en virtud de que las Planillas de Trabajo que las empresas deben presentar ante el Ministerio contienen datos personales de los empleados y de las empresas.
En virtud de la consulta recibida y en cumplimiento de las facultades que le son otorgadas la URCDP por el artículo 34 de la Ley, la Unidad procede a la sustanciación de ésta.

-II-Análisis

II.a. Marco Normativo.

A efectos del encuadre de la presente consulta resulta pertinente referir a las disposiciones legales y reglamentarias que tienen relación directa con el tema.
En primer lugar, debemos analizar la normativa que regula los denominados documentos de control de trabajo establecida por el Decreto N° 108/07, de 22 de marzo de 2007.
En cuanto a las planillas de control de trabajo determina que deben ser llevadas por todas las empresas, sean personas físicas o jurídicas, de cualquier naturaleza, incluso las personas públicas no estatales, que posean personal dependiente.

Los aspectos más relevantes de estas disposiciones para nuestra materia son las que establecen cuál debe

ser el contenido de las planillas de control de trabajo.
El artículo 9° del Decreto dispone que en las planillas deben constar los datos relativos a la identificación de la empresa: razón social, naturaleza jurídica, domicilio y actividad, grupo y subgrupo salarial, número de RUT, número de BPS o caja paraestatal que corresponda y fecha de inicio de actividades. En caso de ser una sociedad comercial debe contener además de la información anterior, el nombre de un director, administrador o gerente y su cédula de identidad.
Respecto a los trabajadores, debe constar: nombre, fecha de nacimiento, sexo, categoría laboral, fecha de ingreso y egreso si la hubiera, salarios en moneda nacional, horarios de trabajo y descansos intermedios y semanales. Por otra parte, la planilla tiene un espacio de "Observaciones" donde es posible anotar todo otro dato de interés para la relación laboral.

Por otra parte, el MTOP tiene como misión "ser el responsable de diseñar, ejecutar, controlar y evaluar la Política Nacional de Transporte en todas sus modalidades y actuando en coordinación con las Intendencias Municipales. Desarrolla la infraestructura nacional necesaria (vial, portuaria, fluvial y ferroviaria) adecuándola a las necesidades de la población, del sector productivo nacional y las políticas de integración regional". 31
Específicamente en materia de transporte, el Decreto Nº 247/997, de 23 de julio de 1997, indica que la Dirección Nacional de Transporte "es responsable del funcionamiento eficiente de los sistemas de transporte nacional e internacional en los modos que las Leyes y Reglamentos le atribuyan competencia, procurando su optimización y potenciando el desarrollo nacional".
De acuerdo con lo proyectado por el MTOP en su Programa sectorial de gobierno para el período 2010-2015, uno de los objetivos para el transporte de cargas por carretera, es la implantación de un sistema de monitoreo y seguimiento del transporte de cargas.

Del análisis de la normativa vigente en la materia y de lo proyectado por el MTOP, el diseño de un Sistema de Información de Transporte de Carga Terrestre y guías de carga forma parte de los cometidos de éste.
Se indica que para el ingreso en las guías es necesario verificar que los profesionales registrados o que estén enviando información, pertenezcan a la empresa correspondiente. Es con este objetivo que el MTOP requiere la información contenida en las planillas de trabajo llevadas por el MTSS.

II.b. Análisis desde la normativa de protección de datos personales.
La Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP) regula en su artículo 17 los derechos referentes a la comunicación de datos.
Establece como principio que los datos pueden ser comunicados con el previo consentimiento del titular de éstos y para el cumplimiento de los fines relacionados directamente con el interés legítimo de su titular.
El artículo establece además en forma taxativa los casos en que no será necesario el consentimiento del titular de los datos para su comunicación. Entre las hipótesis previstas se encuentran los supuestos determinados por el artículo 9º de la Ley.
El mencionado artículo prevé las hipótesis en las cuales no se requiere consentimiento del titular de los datos para el tratamiento de éstos.

31 http://www.mtop.gub.uy/gxpsites/hgxpp001?1,1,18,O,S,0,MNU;E;1;3;11;3;MNU;,

En el caso planteado en la consulta debemos analizar la hipótesis prevista por el artículo 9º literal B) de la Ley. Dicha disposición exceptúa de consentimiento del titular en el caso de que los datos "se recaben para el ejercicio de las funciones propias de los poderes del Estado o en virtud de una obligación legal".
De acuerdo con la normativa mencionada, el MTOP solicita al Ministerio de Trabajo las planillas de trabajo presentadas por las empresas con el objetivo de gestionar el sistema antes mencionado.
El MTOP solicita los datos en virtud del cumplimiento de cometidos específicos que le son asignados por la Ley. Por ello, podríamos concluir que dichos datos se recaban en el marco del ejercicio de sus funciones propias.
Por tanto, en la presente consulta se verifica la configuración de la excepción prevista en el artículo 9° literal B) de la Ley, por lo que la comunicación de datos se considera es legítima en virtud de que el MTOP está ejerciendo funciones propias del organismo.

Por otra parte, correspondería tener en cuenta la excepción dispuesta en el artículo 9º literal C) de la Ley. En él se indican los datos correspondientes a personas físicas que no requieren el previo consentimiento del titular para su tratamiento: nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento.
De acuerdo con lo informado en la consulta se comunicarán únicamente los nombres y apellidos y el documento de identidad de los empleados. En este caso, y de acuerdo a la excepción analizada, se trataría de datos que no requerirían de previo consentimiento del titular para su comunicación.

-III-Conclusiones

Partimos de la base de que en la consulta planteada, resultan aplicables las disposiciones en materia de Protección de Datos Personales reguladas por la Ley Nº 18.331, de 11 de agosto de 2008.
Dentro de sus disposiciones la Ley prevé que para comunicar datos es necesario contar con el consentimiento del titular. Establece además un elenco de excepciones en forma taxativa.
El Ministerio de Transporte y Obras Públicas es un organismo público que en ejercicio de sus funciones, solicita los datos al Ministerio de Trabajo y Seguridad Social, que es quien puede brindarle la información sobre los empleados que tienen las empresas.
De acuerdo con ello, el caso podría quedar incluido en la hipótesis prevista en el artículo 9º literal B) de la Ley, donde se indica que no es necesario el consentimiento del titular cuando se trate de organismos en el ejercicio propio de sus funciones.
También sería de aplicación la excepción contenida en el artículo 9º literal C) que define en forma taxativa cuáles son los datos relativos a las personas físicas que están exceptuados de consentimiento previo del titular de los datos. De acuerdo a esta disposición los datos objeto de la consulta (nombres, apellidos y documento de identidad) no requerirían para su comunicación el previo consentimiento del titular de los datos.
Por último, se recomienda tener en cuenta todos los principios contenidos en la LPDP.

Fdo. Dra. Jimena Hernández
Derechos Ciudadanos

Informe N° 6897 de 11 de noviembre de 2011.
Se informa denuncia derivada de la omisión al rectificar datos personales en una base de datos de una institución bancaria.

INFORME N°		EXPEDIENTE N°
6987	2011	2011-2-10-0000609

Montevideo, 11 de noviembre de 2011.

-I-Antecedentes y resumen de los hechos

La denunciante aduce en varias notas presentadas ante la URCDP, que el BB comunicó a su hermana (de mismo primer nombre y apellido) información personal respecto al préstamo hipotecario que tramitaba ante el mismo.
Afirma que este error derivó de la omisión del Banco de no actualizar o rectificar la información respecto a su teléfono base en tiempo y forma, siendo que ella lo habría comunicado cuando gestionó la tarjeta de crédito ante el mismo banco.

También expresa que, a raíz del suceso presentó una nota de reclamo ante el BB planteando la queja y solicitando toda la información que existiere sobre ella. Sin embargo no consta sello de recibido del Banco en las notas que se adjuntan al expediente.

A raíz de sus afirmaciones el Consejo de la URCDP, de mandato verbal resuelve consultarla acerca de si ha ejercido formalmente el Derecho de Acceso (art. 14).

La Sra. AA contesta que no lo ha hecho porque desconocía el art. 14 y además, con respecto a la "respuesta del Banco frente a mi solicitud durante el período de siete meses en el que realicé los distintos trámites de créditos hipotecarios. A pesar de que consideraba que correspondía se me entregara copia por cada trámite".
En base a lo anterior, la URCDP envía un telegrama (N° 9332) solicitando a BB se agregue toda la documentación pertinente de acuerdo a los hechos denunciados.

-II-Información proporcionada por el BB

Una vez recibido el telegrama de la URCDP, el BB crea un expediente interno GEX N°…, comunicando mediante correo electrónico los datos sobre el trámite iniciado, tanto a la denunciante como a AGESIC, aunque en este último caso en forma errónea ya que el correo electrónico no es correcto y tal información nunca es recibida por la URCDP.

La URCDP continúa con el trámite ignorando el desarrollo del tema a la interna de la institución, dando vista a BB de lo actuado. En dos oportunidades la entidad presenta sus descargos, adjuntando las copias de una serie de correos electrónicos mediante los cuales se comunican con la denunciante y ofrecen enviarle la

información solicitada. La Sra. AA, según consta en uno de ellos, les ruega dejar sin efecto el envío pues prefiere retirarla personalmente.

En sucesivos escritos presentados, BB aduce que la denunciante ha sido omisa a la hora de recoger tal información (por lo menos hasta setiembre fecha en que mantuvo entrevista con el banco), así como respecto de informar a la Unidad sobre todo lo actuado por la institución.
Cabe considerar además que BB ha presentado ante la URCDP, sus bases de datos: "Proveedores", "Clientes y Usuarios", "Personal y Beneficiarios" y "Contrapartes Legales", por lo cual las mismas se encuentran en trámite de inscripción.

-III-Conclusiones y recomendación

En síntesis, si bien cabe inferir que ha existido por parte de BB una comunicación de datos personales originada en el error de un funcionario (art. 17), luego de estudiada toda la información disponible en el expediente, no surgen claros los hechos, ni las circunstancias y plazos en que la Sra. AA ha ejercido sus derechos de acceso, actualización o rectificación (arts. 14 y 15, no aportando la denunciante hasta la fecha nuevos elementos probatorios que sustenten su versión. Es de destacar que se le confirió vista el 7 de octubre del corriente a tales efectos y no presentó descargos.
En razón de ello, cumplidos los plazos otorgados a ambas partes para que adjunten prueba, presenten aclaraciones y/o descargos, se recomienda al Consejo archivar las actuaciones dando vista previa a la denunciante.

Fdo. Graciela Romero
Derechos Ciudadanos

Informe N° 6977 de 9 de setiembre de 2011.

Se informa denuncia sobre falta de logos de videovigilancia en una unidad de transporte de pasajeros.

INFORME N°		EXPEDIENTE N°
6977	2011	2011-2-10-0000523

Montevideo, 9 de noviembre de 2011-
Ref. Denuncia AA c/ BB S.A..

-I-Antecedentes

El 29 de agosto de 2011, el Sr. AA presenta denuncia online ante la Unidad Reguladora y de Control de Datos Personales (en adelante URDCP), debido a que en los coches nuevos de la empresa BB S.A., denominados "METALPAR", hay tres cámaras de seguridad. Según el denunciante, si bien dos de las mismas son para controlar a las personas que descienden del coche, no queda claro la función de la tercer cámara, pues no figura en ningún lugar del coche el logo de videovigilancia correspondiente.

Agrega que en razón de ello desea conocer la función de la cámara del coche N° 92 de BB S.A., y que "si es para filmar ¿por qué no aparece que los datos tomados serán protegidos?".
La URCDP recepciona la denuncia y para un mejor pronunciamiento se da vista al denunciado el 8 de setiembre, quien presenta descargos el 14 de setiembre.

-II-Sobre los descargos presentados por BB

Según los argumentos presentados por BB SA, "la cámara en cuestión es para cuando el bus coloca la reversa y por lo tanto es para total protección de quienes se puedan encontrar tras el vehículo". Agregan que "nada se graba porque no existen computadoras con tal fin".
Sin embargo, la Ing. Viviana García, -en el informe técnico que luce a fojas 21 del expediente- expresa que existen sistemas de cámaras que cuentan con un videograbador y un dispositivo de almacenamiento integrados que no requieren estar conectados a una computadora.

En este caso, las imágenes pueden ser visualizadas por el conductor del ómnibus mediante una o más pantallas. Pero también existen sistemas de este tipo que pueden trasmitir las imágenes a un centro de control desde donde pueden visualizar las imágenes en tiempo real.
En el referido informe finalmente se sugiere solicitar a la empresa BB S.A. que explique con detalle las características y funcionamiento de las cámaras instaladas y el sistema de vigilancia utilizado.
Se procede a dar vista a la empresa del informe técnico citado, solicitándole que amplíe la información respecto al sistema utilizado y la finalidad del mismo.

BB S.A. toma vista de las referidas actuaciones el 22 de setiembre pero pasado el plazo legal correspondiente no ha procedido a proporcionar la información solicitada.

También se procede a dar vista al denunciante de lo informado por BB S.A. en su oportunidad, pero transcurrido el plazo estipulado para ello no ha presentado observaciones al respecto.

-III- Sobre la inscripción de la Base de Datos de BB S.A.

La Ley establece que para que una base de datos se considere legítima es necesario que se encuentre inscripta ante el registro que el órgano de control lleva a estos efectos (Principio de Legalidad, Art. 5º de la Ley). Asimismo, establece la obligación de que todos los organismos públicos, empresas y personas físicas inscriban sus bases de datos (art. 28 y 29 de la LPDP).

A estos efectos, el artículo 1º del Decreto 664/008, de 22 de diciembre de 2009 creó el "Registro de Bases de Datos Personales". Con posterioridad, el Decreto Nº 414/009 estableció un plazo de 90 días para la inscripción de las bases de datos ya existentes (plazo que se venció el 14 de diciembre de 2009) o 90 días desde el inicio de actividades para las nuevas bases.

-IV-Conclusiones

La información que obra en el expediente no permite afirmar que se esté frente a una violación de la Ley N° 18.331 y su Decreto Reglamentario, sin embargo corresponde tener presente que la empresa ha sido omisa al no ampliar la información solicitada a la URCDP en el marco de sus competencias legales.
Por otra parte, se sugiere al Consejo de la URCDP que intime a BB S.A. a inscribir sus bases de datos con el fin de dar cumplimiento a lo establecido en el art. 10 de la norma.

Fdo. Graciela Romero
Derechos Ciudadanos

Informe N° 6982 de 10 de noviembre de 2011.
Se informa denuncia sobre inclusión de datos personales en una base de datos de morosos.

INFORME N°		EXPEDIENTE N°
6982	2011	2011-2-10-0000596

Montevideo, 10 de noviembre de 2011.
Ref. AA c/ BB S.A..

-I- ANTECEDENTES

I.A. Con fecha 18 de Setiembre de 2011, el Sr. AA presentó ante la Unidad Reguladora y de Control de Datos Personales una denuncia contra la empresa BB S.A. en virtud de encontrarse como deudor en dicha entidad. La situación fue constatada por el denunciante al realizar una operación en Antel.

I.B. Solicita se inicien las actuaciones administrativas correspondientes. En virtud de las cuales se procede a dar vista de la denuncia a la empresa BB S.A. a través de telegrama colacionado. Con fecha 30 de setiembre de 2011, se presenta a tomar vista.
I.C. El día 07 de Octubre del corriente la empresa BB S.A. presenta sus descargos, procediéndose a dar vista de éstos al denunciante. En virtud de ello, el denunciante concurre a tomar vista y presenta descargos.

-II-ANÁLISIS DE LA DENUNCIA

II.A. Hechos. El denunciante afirma que en ocasión de solicitar un servicio en Antel, no pudo concretarlo dado que se le comunicó que se encontraba en BB. Afirma que la deuda mencionada ya había sido paga con fecha 4 de octubre de 2010. Agrega que debió acreditar el pago de la mencionada a través de las facturas que conservaba y que finalmente accedió al servicio solicitado.

Por otra parte, alega que existe una contradicción entre la información que figura en Antel y la que figura en BB.
Por su parte, la empresa BB., alega que respecto al Sr. AA no surge ningún registro de operación incumplida y que no ha ejercido frente a ésta, los derechos de acceso, rectificación o actualización de datos.

II.B. Marco legal. El artículo 22 de la Ley Nº 18.331 dispone que “Los datos personales relativos a obligaciones de carácter comercial de personas físicas solo podrán estar registrados por un plazo de cinco años contados desde su incorporación. En caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original. Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción”.

En mérito a lo expuesto, el consultante debería esperar al vencimiento del plazo por el cual es legítimo mantener el registro de la deuda, y efectuar luego de esa fecha una solicitud de acceso ante BB S.A. -al amparo de lo previsto por el artículo 14 de la LPDP- a fin de constatar que se haya eliminado la información. Se debe tener presente que de los descargos presentados por BB S.A. surge que no se cuenta con datos del denunciante en la base de datos que administra. Por otra parte, el denunciante puede ejercer su derecho de acceso y presentarse a efectos de obtener su historia crediticia que forme parte de la base de datos de la empresa.

Por otra parte, el derecho referido puede ser ejercido frente a la empresa Antel a efectos de consultar cuáles son los datos que sobre sí figuran y constatar que se ha modificado el dato erróneo sobre el estado de su deuda.Para el ejercicio del derecho de acceso se podrá utilizar el modelo diseñado por la URCDP a tales efectos, ingresando, a través de su sitio web, al link: http://www.datospersonales.gub.uy/sitio/pdf/Formulario_para_ejercer_el_derecho_de_acceso.pdf

-III-CONCLUSIONES

III.A. En atención a la denuncia presentada y a los descargos formulados por las partes, no surge que exista una conducta violatoria de las disposiciones de la Ley Nº 18.331.

III.B. Se recomienda al denunciante, en virtud de los descargos formulados por BB S.A., que ejerza el derecho de acceso de acuerdo con lo establecido en el artículo 14 de la Ley Nº 18.331 frente a la empresa, a efectos de que se le informe todo el historial de crédito que sobre si existe en la base de datos por ellos administrada. Si surge un registro de obligación incumplida, debe esperar el vencimiento del plazo por el cual es legal mantener el registro, y efectuar luego de esa fecha una solicitud de acceso ante BB S.A. -al amparo de lo previsto por el artículo 14 de la LPDP- a fin de constatar que se haya eliminado la información.

III.C. Se recomienda además, que el denunciante ejerza su derecho de acceso ante Antel y corrobore si se ha modificado el dato erróneo.
Es todo cuanto tengo que informar.

Fdo. Dra. Jimena Hernández
Derechos Ciudadanos

Informe N° 7010 de 18 de noviembre de 2011.

Se informa consulta relativa al tratamiento de datos personales de imagen por parte de la prensa.

INFORME N°		EXPEDIENTE N°
7010	2011	2011-2-10-0000835

Montevideo, 18 de noviembre de 2011

Sobre la consulta realizada por el Director Ejecutivo de la Agencia Ing. José Clastornik respecto al uso que hace la prensa de las imágenes personales, por ejemplo accidentados, victimas o victimarios, y cómo aplica la Ley de PDP, cabe realizar las siguientes puntualizaciones:

-I-El art. 4° de la Ley N° 18.331, entre sus definiciones, establece que se entiende por dato personal a la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. Por lo tanto la imagen constituye un dato personal.
Dicho artículo también define a la comunicación de datos, como toda revelación realizada a una persona distinta del titular, así como al tratamiento de datos a las 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.

Por otra parte, en su artículo 9° establece que dicho tratamiento de datos es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse o, en su defecto, acreditar que los datos provienen de fuentes accesibles al público o bien que existe una Ley que ampara ese tratamiento o una relación contractual o negocial entre el titular de los datos y el responsable del tratamiento.
En nuestro país además de la Ley N° 18.331, hay que tener presente el Código de la Niñez y la Adolescencia del 2004, que en su Artículo 11 sobre el derecho a la privacidad de la vida establece que todo niño y adolescente tiene derecho a que se respete la privacidad de su vida y tiene derecho a que no se utilice su imagen en forma lesiva, ni se publique ninguna información que lo perjudique y pueda dar lugar a la individualización de su persona (subrayado nuestro).

Esto último refiere a una protección especial que nuestro legislador, -de acuerdo con lo establecido en la Convención de Derechos del Niño de 1989-, ha decidido otorgar a las personas que poseen menos de 18 años de edad.

-II-Ahora bien, en la consulta de referencia corresponde realizar el análisis ponderando especialmente los derechos en juego: el derecho a la protección de datos personales y el derecho a la libertad de expresión y de información, ambos de rango constitucional.

En este sentido considerando lo expresado tanto en fallos judiciales nacionales como la opinión de la Corte Interamericana de Derechos Humanos32, hay que tener presente que no corresponde legalmente aplicar el "instituto de la censura previa", pues los instrumentos jurídicos (Constitución Nacional y Convención Interamericana de Derechos Humanos, entre otros), obligan a realizar una distinción entre censura previa y responsabilidades ulteriores, encontrándose la primera de ellas prohibida.

No obstante ello es posible y necesario realizar la ponderación de ambos derechos. En este sentido, la Agencia Española de Protección de Datos33, -citando al Tribunal Constitucional Español-, expresa que estamos ante una una cuestión estrictamente de colisión entre la libertad de información y el derecho a la propia imagen, con el consiguiente poder de disposición de la persona sobre su propia imagen.

Entonces, si bien las personas tienen el poder de decisión sobre la difusión de su propia imagen como dato personal, (...) es un derecho que no es absoluto, que debe ceder llegado el caso ante la prevalencia de otros derechos y libertades constitucionalmente reconocidos y protegidos, como es la libertad de información, siempre que se ejerza ésta dentro de los límites ya reseñados y determinados por la jurisprudencia del Tribunal Constitucional en relación al derecho a la propia imagen, a saber: veracidad e interés general, que deberán ser ponderados caso a caso según sus circunstancias.

Agrega que "el tratamiento de los datos personales debe estar (...) sujeto a un principio de proporcionalidad, (…) datos personales adecuados, pertinentes, no excesivos y circunscritos a la finalidad que tiene el reportaje, que no es otra que ilustrar la información aportada(subrayado nuestro).
Por ende, los medios de comunicación deben valorar la necesidad de que su actuación se dirija a conciliar, en mayor medida, el derecho a la libertad de información con la aplicación de los principios de protección de datos personales, ambos derechos fundamentales.

En primer lugar debe ponderarse escrupulosamente la relevancia pública de la identidad de las personas afectadas por el hecho noticiable para, en el caso de que no aporte información adicional, evitar la identificación mediante la inserción en prensa de su imagen sin su consentimiento (subrayado nuestro).

32 Por ejemplo sentencia Juzgado Letrado en lo Civil de 8° Turno. Fecha: 7 de octubre 2008. Jueza Dra María Esther Gradín. Los padres de un joven que 10 años atrás había sido autor de dos homicidios, pidieron se prohibiera a un canal de televisión la realización de un programa sobre el caso.

En el ámbito de la Corte Interamericana el documento referente es la OPINIÓN CONSULTIVA OC-5/85 del 13 de noviembre de 1985 de la CORTE INTERAMERICANA DE DERECHOS HUMANOS sobre la Colegiación Obligatoria de Periodistas (arts. 13 y 29 de la Convención).

33 Expediente Nº: E/00777/2007. Resolución de archivo de actuaciones. Mayo 2009. De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad DIARIO EL PAIS, S.L. en virtud de denuncia presentada ante la misma por Dª. E.E.E. http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2009/common/pdfs/E-00777-2007_Resolucion-de-fecha-04-03-2009_Art-ii-culo-20-CE.pdf)

Por tanto para cumplir con ello y no incurrir en una eventual vulneración de derechos, los medios de comunicación deberían aplicar una disociación del datos (Art. 4° G), esfumando o pizzelando el rostro de los involucrados en los casos en que no existe un interés público que transforme en relevante la identidad de una persona, o en los casos en que develar la imagen de una persona puede resultar lesivo, excesivo y no adecuado a la finalidad que posee la noticia.

En este caso si bien, como ya hemos expresado, no es posible aplicar censura previa, toda persona que considere que se ha vulnerado su derecho a la imagen y por ende a la protección de sus datos personales causándole un daño, podrá hacer valer sus derechos exigiendo la responsabilidad de quien corresponda.

Fdo. Graciela Romero
Derechos Ciudadanos

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

Andes 1365 piso 8, Montevideo, Uruguay Te l.: (+598) 2901 2929 ext. 1352
Email: info @datospersonales.gub.uy
www.datospersonales.gub.uy