UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

2014

Resoluciones Dictámenes e Informes

agesic
agencia de gobierno electrónico
y sociedad de la información

PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

2014

Resoluciones Dictámenes e Informes

agesic
agencia de gobierno electrónico y sociedad de la información

PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY

INDICE

RESOLUCIONES

PAG.

DICTÁMENES

INFORMES

RESOLUCIONES

Resolución Nº 16 de 13 de febrero de 2014.

SSe resuelve denuncia relativa a la utilización de datos personales sin autorización del titular, imponiéndose sanción a las empresas infractoras.

RESOLUCION Nº		EXPEDIENTE Nº
16	2014	2011-2-10-0001065

Montevideo, 13 de febrero de 2014

VISTO:

La denuncia presentada por la Sra. AA contra BB por utilización de sus datos personales sin autorización, con el fin de enviarle una tarjeta de crédito Visa, sin haberla solicitado.

RESULTANDO:

I) Que la Unidad confirió vista a la parte denunciada y a CC en su calidad de emisora de la tarjeta de crédito y realizó informes al respecto.

II) Que BB manifestó que la tarjeta de crédito enviada es una pieza promocional cuya emisión y envío se encuentra amparada en la relación contractual mantenida con la denunciante y en la aceptación explícita de su Política de Privacidad, por lo que no consideran haber contravenido el artículo 8 de la Ley N° 18.331 de 11 de Agosto de 2011 (LPDP). Señaló asimismo, que no le corresponde probar el consentimiento, existiendo en la especie inversión de la carga de la prueba.

III) Que se presentó CC e informó que la tarjeta de crédito es una pieza promocional que se enmarca en una campaña desarrollada por BB; que su envío a la denunciada se encuentra respaldado por la aceptación explícita de la Política de Privacidad del denunciado, que le permite contactarse con el cliente e informarle de nuevos productos o servicios, por lo que entiende que no se vulneró el principio de finalidad, que para su emisión se requieren datos exonerados del previo consentimiento informado, como ser nombres, apellidos, cédula de identidad y domicilio, no existiendo por tanto infracción al artículo 17 de la LPDP.

CONSIDERANDO:

I) Que se está ante una situación alcanzada por la Ley N° 18.331 y su Decreto reglamentario N° 414/009.

II) Que la tarjeta de crédito no puede asimilarse a una pieza promocional, desde que se trata de un negocio jurídico complejo; su emisión y envío tampoco puede entenderse incluido en la finalidad del contrato de servicio que une a BB y a AA, ni fundarse en la cláusula denominada de “Recopilación y uso de información” de la Política de Privacidad aceptada por la denunciante.

III) Que el artículo 6 in fine del decreto N° 414/009 dispone que corresponderá al responsable de la base de datos o el tratamiento recabar y guardar la prueba de la existencia del consentimiento o de la negativa a darlo, por parte del titular, a través de cualquier medio conforme a derecho.

IV) Que el contrato de emisión de tarjeta de crédito es un contrato comercial mediante el cual el emisor (CC) concede un crédito al usuario (AA); que acorde las estipulaciones contractuales vigentes de CC, inscriptas ante la Dirección General de Comercio conforme decreto N° 78/2002, la línea de crédito se concede con anterioridad a la suscripción del contrato mediante estudio de información relativa al solicitante; que no puede sostenerse que dicho estudio y concesión se base únicamente en los datos contenidos en el artículo 9 C de la LPDP como alega dicha empresa, por lo que existió comunicación de otros datos en contravención del artículo 17 de la Ley de Protección de Datos.

V) Que BB ha infringido las disposiciones relativas a la finalidad y comunicación de datos, contenidas en los artículos 8 y 17 de la LPDP.

VI) Que CC ha infringido las disposiciones relativas a la comunicación, en tanto destinatario sujeto a las mismas obligaciones legales y reglamentarias que el emisor.

VII) Que según lo establece el artículo 5 de la resolución N° 320/2011 de 17 de marzo de 2011, se considera infracción grave tratar o usar datos personales vulnerando los principios, derechos y garantías consagradas en la LPDP y su reglamentación.

ATENTO:

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

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Sancionar con 12.001 UI a BB por infracción a las disposiciones relativas a la finalidad y comunicación de datos, contenidas en los artículos 8 y 17 de la Ley N° 18.331.
2. Sancionar con 12.001 UI a CC por infracción a las disposiciones relativas a la comunicación de datos, en tanto destinatario sujeto a las mismas obligaciones legales y reglamentarias que el emisor.
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 18, de 13 de febrero de 2014.

Se resuelve denuncia por instalación de cámaras de video vigilancia sin cumplir con el deber de de informar del artículo 13 de la Ley Nº 18.331.

RESOLUCION No.		EXPEDIENTE No.
8	2013	2013-2-10-0000185
		2013-2-10-0000196
		2013-2-10-0000206
		2013-2-10-0000207
		2013-2-10-0000222
		2013-2-10-0000229
		2013-2-10-0000242
		2013-2-10-0000244

Montevideo, 13 de febrero de 2014

VISTO:

Las denuncias presentadas contra AA S.A. (en adelante AA) y BB S.A. (en adelante BB), por recibir llamadas en sus domicilios, en algunos casos en horas de la madrugada, sin haber prestado el consentimiento, y por la falta de opción para poder elegir u oponerse a la comunicación de sus datos.

RESULTANDO:

I) Que todos los denunciantes recibieron un mensaje grabado, mediante el cual se los identifica por sus nombres completos (en algunos casos con los dos nombres y los dos apellidos), y se les avisa que sus datos serán comunicados a BB si en 48 horas no llaman al 2908XXXX (otra contestadora).

II) Que los denunciantes que recibieron la comunicación en horas impropias (la mayoría en la madrugada), alegan haber sido perturbados en la paz de su hogar, así como manifiestan que el número de teléfono receptor no se encuentra a su nombre a pesar de que la llamada fue dirigida hacia ellos.

III) Que algunos de los denunciantes manifestaron inconvenientes en comunicarse al número indicado.

IV) Que BB manifestó que la empresa AA le presta un servicio a través del cual realiza llamadas telefónicas a potenciales clientes, y que el receptor de la llamada posee el derecho de negarse a la comunicación de sus datos personales a través de una gestión telefónica, pero que debido a una incidencia en el marcador automático de AA se realizaron llamados fuera de los horarios habituales.

V) Que AA admite haber realizado las llamadas en cumplimiento de lo solicitado por la URCDP en la Resolución N° 604/2012, mediante la cual se autorizó la inscripción de su base de Prospección Comercial y se dispuso que en todos los casos, antes de comunicar los datos al cliente del servicio, AA debía informar a los titulares de los datos en el marco del artículo 13 de la Ley N° 18.331.

VI) Que dicha base contiene datos provenientes de fuentes públicas de información, así como datos identificatorios, que no requieren el previo consentimiento informado, remarcando

que se trata de una base distinta de la crediticia.

VII) Que lamenta que las llamadas hayan generado molestias por lo impropio de la hora, aclarando que se debió a un error imprevisible en los sistemas del proveedor contratado, la empresa CC SRL (en adelante CC), que hizo que los llamados automáticos se activaran fuera del horario pactado, aclarando que advertido el error, en forma inmediata se tomaron medidas para atender consultas y quejas, y se procedió a suspender la comunicación de los datos en el marco de esta campaña.

CONSIDERANDO:

I) Que se está 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 el derecho a la protección de datos personales es un derecho humano presente en nuestro ordenamiento jurídico a través del artículo 72 de la Constitución de la República y de reconocimiento legal por el artículo 10 de la Ley. En su mérito, las conductas denunciadas que involucran limitaciones en su goce, fundadas en la posibilidad del tratamiento de datos sin consentimiento de su titular con fines de prospección comercial, corresponde se valoren conforme a los criterios interpretativos aplicables en general en materia de derechos fundamentales.

III) Que si bien AA alega que se produjo “un error imprevisible en los sistemas del proveedor contratado a estos efectos”, y que advertido el error se tomaron medidas en forma inmediata, surge de obrados la reiteración en el tiempo del mismo suceso. A fs. 30 del expediente 2013-2-10- 0000196, AA adjunta reporte del problema con fecha 6 de Mayo 2013 y que posteriormente se recibieron 6 denuncias que refieren a llamadas recibidas los días 14, 15, 22, 23, 29 y 31 de Mayo de 2013 (expedientes 207, 206, 222, 229, 242 y 244 de 2013, respectivamente).

IV) Que en cuanto al deber de informar, AA, al ir más allá de lo solicitado por esta Unidad, emitió una comunicación confusa, pasible de mal interpretarse por sus destinatarios como portadora de un consentimiento tácito y consecuente silencio positivo.

V) Que además AA omitió declarar ante esta Unidad a CC como encargado de tratamiento, de acuerdo a lo solicitado en los artículos 29 de la Ley N° 18.331 y 20 del decreto N° 414/009, que indican que los responsables de las bases deberán mantener actualizados los datos inscriptos en el Registro, comunicando trimestralmente las actualizaciones.

VI) Que debido a que los datos no llegaron a comunicarse a BB, se considera improcedente la prosecución de estas actuaciones a su respecto.

VII) Que en definitiva, el denunciado en aplicación de su modelo de negocio y en uso de su base de Prospección Comercial, provocó molestias en personas que expresamente eligieron no figurar en guía para no ser contactadas. No obstante ello, surge del Exp. N° 3540/2010, que AA consultó acerca de la implementación de su modelo de negocios, el cual resultó aprobado en su momento, bajo los parámetros legales vigentes.

VIII) Que esta Unidad estima que las reformas introducidas a la Ley, determinan que el

denunciado deba revisar y adecuar su modelo de negocio y base de Prospección Comercial a la luz del dictamen N° 01/2014, de 05 de febrero de 2014, interpretativo del artículo 9 bis.

ATENTO:

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

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Indicar a AA SA que debe revisar y adecuar su modelo de negocio y base de Prospección Comercial a la luz del dictamen N° 01/2014, interpretativo del artículo 9 bis.
2. Notifíquese, publíquese y oportunamente archívese.
3. Notifíquese y publíquese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 25, de 13 de marzo de 2014.

Se resuelve denuncia por incumplimiento del derecho de acceso regulado en el artículo 14 de la Ley Nº 18.331.

RESOLUCION Nº		EXPEDIENTE Nº
25	2014	2013-2-10-0000129
		2013-2-10-0000387
		2013-2-10-0000501
		2013-2-10-0000502
		2014-2-10-0000006
		2014-2-10-0000012

Montevideo, 16 de mayo de 2013

VISTO :

Las denuncias presentadas por AA contra la Facultad BB de la UDELAR, por incumplimiento del derecho de acceso.

CONSIDERANDO:

I) Que en algunos casos, se constató que el denunciante ejercitó su derecho sin respetar los plazos del artículo 14 de la Ley N° 18.331 de 11 Agosto de 2008, por no mediar justificación de un nuevo interés legítimo.

II) Que asimismo surge de obrados, que en algunos casos la Facultad BB de la UDELAR respondió la solicitud de acceso fuera de los plazos legales.

III) Que deviene imperativo que dicha Facultad adecue su proceder a la normativa sobre protección de datos, a cuyos efectos será incluida en el Plan de Auditorías 2014 de esta Unidad.

ATENTO:

A lo expuesto y a lo previsto en las normas aplicables,

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Exhortar a AA a ejercitar su derecho de acceso conforme las disposiciones del artículo 14 de la Ley N° 18.331.
2. Exhortar a la Facultad BB de la UDELAR a respetar los plazos legales para el amparo del referido derecho.
3. Incluir a la referida Facultad en el Plan de Auditorías 2014 de esta Unidad.
4. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución Nº 28, de 13 de marzo de 2014

Se resuelve denuncia relativa a la falta de adecuación a la Ley de un sistema de registro de datos.

RESOLUCIÓN N°		EXPEDIENTE N°
28	2014	2013-2-10-0000377

Montevideo, 13 de marzo de 2014

VISTO:

La denuncia presentada por la Sra. AA por haberse inscripto a una carrera a través del sitio web http://www.BB.gub.uy/ y advertir con posterioridad, que al ingresar su Cédula de Identidad, se despliegan todos los datos previamente ingresados tales como teléfono celular, correo electrónico y sociedad médica.

RESULTANDO:

I) Que se confirió traslado a BB del Ministerio de Turismo y Deportes (en adelante e indistintamente BB), titular del registro del nombre de dominio, solicitándole que informara si es responsable de la base de datos solicitados a los interesados y número de inscripción ante esta Unidad, así como que acreditara el cumplimiento del deber de información, el ejercicio de los derechos de acceso, rectificación, actualización, inclusión o supresión y el consentimiento expreso y escrito de los titulares para recabar sus datos de salud, de acuerdo con lo dispuesto en los artículo 13, 14, 15, y 18 de la Ley N° 18.331 de 11 de Agosto de 2008.

II) Que evacuado el traslado, BB expresó haber contratado una empresa a efectos de realizar el registro y recabar la información de los participantes. En relación al registro de sus

bases de datos, manifestó que por ser temporales, entiende que no corresponde su inscripción y que las modificaciones de la información pueden solicitarse a través del BB@gmail.com que se encuentra en la sección contacto del sitio de la carrera. Agrega que no colecta datos de salud.

CONSIDERANDO:

I) Que la puesta a disposición de los datos realizada por BB, se enmarca en la definición legal de comunicación de datos personales dada por la Ley de Protección de Datos Personales, desde que la consulta puede realizarla cualquier persona distinta del titular de los datos y por tanto debe contar con el previo consentimiento informado de sus titulares, salvo excepciones.

II) Que el número de celular, correo electrónico y sociedad médica, no pueden enmarcarse en ninguna de las excepciones previstas, así como tampoco puede sostenerse que su comunicación responda a intereses legítimos del emisor y del destinatario.

III) Que BB recabó y comunicó datos sensibles sin cumplir las exigencias normativas, que disponen la necesidad del consentimiento expreso y escrito del titular para su tratamiento y el consentimiento expreso para su comunicación.

IV) Que los datos tratados no pueden ser utilizados para finalidades distintas o incompatibles a las que motivaron su obtención y el caso en estudio presenta una clara discrepancia entre la finalidad de registro (para participar en una carrera) y la consulta de datos.

V) Que asimismo se verifica incumplimiento del artículo 13 de la Ley N° 18.331 que regula el derecho de información frente a la recolección de datos.

VI) Que el hecho que una base de datos se mantenga por un lapso corto de tiempo no exime a BB de la obligación de registro ante esta Unidad, conforme los artículos 24 de la LPDP y 15 y siguientes del decreto N° 414/009.

ATENTO:

A lo expuesto y a lo previsto en las normas aplicables,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Hacer saber a BB que el sistema de registro en estudio no se ajusta a las disposiciones de la Ley N° 18.331, en virtud de no cumplir con lo dispuesto por los artículos 9, 13, 18 y 24 de la norma y por desvirtuar la finalidad de registro en consulta.
2. Exhortar a BB la inmediata adecuación de sus procesos de inscripción en línea a las disposiciones de la Ley N° 18.331, poniendo especial atención al tratamiento de la información de carácter sensible.
3. Intimar a BB el registro de las bases de datos de las que sea titular, en el plazo de 30 días corridos.
4. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 32, de 13 de marzo de 2014.

Se resuelve denuncia relativa a la instalación de cámaras de videovigilancia que apuntan hacia el balcón del apartamento de la denunciante.

RESOLUCION Nº		EXPEDIENTE Nº
32	2014	2012-2-10-0000903

Montevideo, 13 de marzo de 2014

VISTO:

La denuncia presentada por AA contra BB, por instalar una cámara de videovigilancia que apunta hacia el balcón de su domicilio.

RESULTANDO:

I) Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista en varias oportunidades a la parte denunciada, pero no se ha presentado a efectos de aportar las aclaraciones pertinentes.

. II) Que asimismo se ha realizado inspección en el lugar, constatando la existencia de una cámara de seguridad que apunta hacia el balcón del domicilio de la denunciante, así como de otras cámaras que se encuentran ubicadas en diferentes puntos del edificio con la finalidad de mantener la seguridad .

III) Que se ha notificado a la administración del edificio, la que se presenta a inscribir las bases de datos de videovigilancia del mismo, así como para aclarar que la Asamblea de Copropietarios si bien no ha autorizado la instalación de la cámara objeto de la denuncia, conoce de su existencia debido a temas de inseguridad, y ofrecen como posible solución a la denunciante, la posibilidad de colocar una mampara en el balcón (de similares características a la que ya está instalada en otra unidad), cuyo costo sería asumido entre todos.

CONSIDERANDO:

I) Que se está 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 la imagen es un dato personal cuyo tratamiento debe estar sujeto a la normativa de protección de datos personales.

III) Que en el caso de la cámara que origina la denuncia, cabe indicarse que la misma vulnera los principios de legalidad, finalidad y proporcionalidad establecidos en la norma (arts. 6°, 7° y 8°), por lo cual debería modificarse su ubicación de forma que no se enfoque exclusivamente hacia el balcón del apartamento lindero.

IV) Que en definitiva, no surge de las actuaciones que la videovigilancia denunciada esté amparada por el marco legal vigente ni que se ajuste a los principios que rigen la protección de datos personales, a lo que se suma que el denunciado no ha colaborado en ningún momento con esta Unidad ni han aportado información que permita aclarar su situación.

V) Que en definitiva, corresponde considerar, que se incurre por parte del denunciado en un tratamiento que vulnera lo establecido en la LPDP, arts. 1°, 6°, 7°, 8°, 9°, 13 y 25.

ATENTO:

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

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1.- Sancionar con multa de 1.000 UI a BB por infracción a la Ley Nº 18.331.

2.- Notifíquese, publíquese y oportunamente archívese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 39, de 27 de marzo de 2014.

Se resuelve denuncia relativa al cumplimiento fuera de plazo del derecho de supresión de datos.

RESOLUCION Nº		EXPEDIENTE Nº
39	2014	2014-2-10-0000044

Montevideo, 27 de marzo de 2014

VISTO:

La denuncia presentada por AA contra BB por enviarle correos promocionales a pesar de haber solicitado lo contarlo.

RESULTANDO:

Que conferido traslado a BB manifestó que el denunciante ejerció su derecho de retiro o bloqueo con fecha 24/01/2014, y que una demora en el procesamiento informático provocó que recibiera un correo posterior con fecha 30/01/2014. Asegura que los datos del denunciante han sido eliminados “de todas las categorías de productos en relación a las cuales el Banco realiza publicidad a través del envío de mails”.

CONSIDERANDO:

I) Que el artículo 21 de la Ley N° 18.331, establece que el titular de datos contenidos en bases utilizadas con fines promocionales, tiene derecho de solicitar el retiro o bloqueo de sus datos, en cualquier momento.

II) Que surge de obrados, que el denunciado amparó el derecho fuera de plazo.

III) Que BB tiene registradas sus bases de datos ante esta Unidad.

ATENTO:

A lo expuesto y a lo previsto en las normas aplicables,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Exhortar a BB a que ajuste sus sistemas informáticos y capacite a sus recursos humanos, para cumplir con los tiempos y requerimientos de la Ley N° 18.331.
2. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 60, de 24 de abril de 2014.

Se resuelve denuncia relativa al cumplimiento fuera de plazo del derecho de acceso a datos personales regulado en el artículo 14 de la Ley Nº 18.331.

RESOLUCION Nº		EXPEDIENTE Nº
60	2014	2012-2-10-0000923

Montevideo, 24 de abril de 2014

VISTO:

La denuncia presentada por el Sr. AA contra BB, por no brindarle acceso en plazo, a la información personal que ha solicitado.

RESULTANDO:

I) Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista a todas las partes.

II) Que BB manifiesta que el denunciante siempre ha tenido la posibilidad de acceder a toda su información contenida en diversos expedientes en el marco de lo previsto en el Decreto 500/91 (arts. 12 y 77 de dicho decreto).

III) Que además considera que no aplica al caso esta Ley, pues no habría una base de datos en sí, sino un conjunto de expedientes con el objeto de que el Departamento de Certificaciones Médicas, pueda determinar la aptitud física y mental del funcionario.

CONSIDERANDO:

I) Que se está 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 esta norma consagra un sistema de protección específico para el derecho a la protección de datos (art.1° de la Ley y art. 72 de la Constitución), del cual se desprenden un conjunto de derechos y obligaciones con diferente alcance y naturaleza jurídica (arts. 14, 15 y 16), que deben distinguirse de otros similares que aplican al ámbito administrativo, y se plasman básicamente en el Decreto 500/91.

III) Que también existe en el ámbito de la salud normativa específica que alcanza a

BB y garantiza derechos a los usuarios y pacientes del sistema, como es caso de la Ley N° 18.335.

IV) Que en el art. 14 de la Ley N° 18.331 se consagra el derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas, en un plazo de cinco días hábiles y que vencido éste sin que el pedido sea satisfecho, o si fuera denegado por razones no justificadas, quedará habilitada la acción de habeas data.

V) Que si bien es cierto que el Decreto 500/91 determina las reglas para el acceso a los expedientes administrativos, se trata de un acceso diferente al derecho que se consagra en el art. 14, en razón de su alcance y finalidad.

VI) Que en definitiva, debe proporcionarse acceso en el plazo de 5 días, a toda información que se posea y se relacione con el denunciante, por ejemplo al listado de expedientes que se hayan iniciado o se tramiten contra él, así como a toda otra documentación de diversa índole y en cualquier soporte, que no esté contenida en dichos expedientes.

VII) Que además, la Ley aplica al tratamiento de datos "registrados en cualquier soporte" (art. 3° ámbito objetivo), por ello no necesariamente debe presuponerse la existencia de una base, en el sentido de un conjunto organizado de datos, para garantizar y proteger el derecho que consagra la norma.

VIII) Que a su vez, en el artículo 6° se prevé que la formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, por lo cual corresponde indicar que el organismo denunciado aún no ha cumplido con tal obligación.

IX) Que en cuanto denunciante, hay que tener presente que puede ejercer en forma gratuita su derecho a intervalos de 6 meses, salvo interés legítimo que se debe acreditar, y que respecto al acceso a su historia clínica, corresponde aplicar la norma específica, o sea la Ley N° 18.335 art. 18 Literal D y art. 33 del Decreto N° 274/2010.

ATENTO:

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

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Sancionar con observación a BB por infracción a la Ley Nº 18.331, arts. 6° y 14.
2. Intimar la inscripción de sus bases de datos en un plazo de 30 días.
3. Advertir al denunciante acerca del plazo de seis meses previsto en el art. 14 de la Ley 18.331.
4. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 66, de 30 de abril de 2014.

Se resuelve denuncia relativa al envío de una comunicación por correo electrónico a varios interesados sin realizar copia oculta de los destinatarios.

RESOLUCION N°		EXPEDIENTE N°
66	2014	2013-2-10-0000470
		2013-2-10-0000471
		2013-2-10-0000485

Montevideo, 30 de abril de 2014

VISTO:

Las denuncias presentadas contra AA por comunicación de datos a terceros.

RESULTANDO:

I) Que se dio trámite a éstas, confiriendo oportunidad a la denunciada para que formulara sus aclaraciones y explicara qué sucedió al realizar el envío sin copia oculta de los correos a los postulantes del concurso no seleccionados.

II) Que en las dos comparecencias de aclaraciones, la denunciada expresó que se trató de un error involuntario el envío de los correos sin copia oculta, que el correo electrónico no es un dato personal y que no identifica a las personas (fojas 59 y 79).

III) Que la base de datos se encuentra inscripta al haberse utilizado la base de datos de BB.

CONSIDERANDO:

I) Que realizado el estudio de la normativa aplicable el hecho denunciado configura la hipótesis de comunicación de datos personales incumpliendo el artículo 17 de la Ley Nº 18.331, ya que el correo electrónico es un dato personal de acuerdo con el artículo 4º literal D).

II) Que el hecho denunciado se ha producido en reiteradas ocasiones y que se tipifica como infracción por lo que se aplicará el artículo 35 de la Ley en cuanto a las sanciones a recaer.

ATENTO:

A lo expuesto y lo dispuesto por los artículos 4º literal D), 9º, 17 y 35 de la Ley N° 18.331

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Observar a AA por la infracción al artículo 17 de la Ley Nº 18.331 (comunicación de datos personales) emergente de obrados.
2. Notifíquese y publíquese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 67, de 30 de abril de 2014.

Se resuelve denuncia por el envío de correo electrónico no deseado en el cual se ofrece la venta de base de datos.

RESOLUCION Nº		EXPEDIENTE Nº
67	2013	2011-2-10-0000167
		2011-2-10-0000168
		2011-2-10-0000169
		2011-2-10-0000170
		2011-2-10-0000905
		2012-2-10-0000080
		2012-2-10-0000271
		2012-2-10-0000429
		2012-2-10-0000505
		2012-2-10-0000745
		2012-2-10-0000842
		2012-2-10-0000872
		2012-2-10-0000967
		2013-2-10-0000027
		2013-2-10-0000028

Montevideo, 30 de abril de 2014

VISTO:

Las denuncias presentadas contra AA, por el envío de correos electrónicos no deseados ofreciendo la venta de bases de datos.

CONSIDERANDO:

I) Que se está ante una situación alcanzada por la Ley N° 18.331 de 11 de agosto de 2008 (en adelante LPDP), y su Decreto reglamentario N° 414/009 de 31 de agosto de 2009.

II) Que se constató la existencia de bases de datos (las ofrecidas) que no se encuentran inscriptas ante esta Unidad.

III) Que dadas las circunstancias emergentes de obrados, por Acta N° 20 de 1 de Agosto de 2013, el Consejo Ejecutivo de la Unidad decidió intimar al denunciado a inscribir sus bases de datos de correos electrónicos, a que indicara la procedencia de las direcciones electrónicas que las conforman y a que informara sobre el mecanismo habilitado para que los titulares ejerzan el derecho de retiro o bloqueo consagrado en el artículo 21 de la LPDP, bajo apercibimiento de ser sancionado.

IV) Que intimado notarialmente, el denunciado ha incumplido con lo solicitado.

V) Que en definitiva, se ha incurrido por parte del denunciado en un incumplimiento del deber de registro de base de datos establecido en la Ley N° 18.331 así como de proporcionar la información referenciada por parte de esta Unidad (art. 34 “E” de la citada Ley y a lo establecido en la Resolución 320/2011 de 17-III-2011).

VI) Que en cuanto a otros aspectos emergentes de obrados, corresponderá continuar con su investigación y análisis.

ATENTO:

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

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES
RESUELVE:

1. Sancionar con multa de UI 15.000 (Unidades Indexadas quince mil) a AA, por infracción a la Ley N° 18.331.
2.- Notifiquese, publiquese y vuelva.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 69, de 15 de mayo de 2014.

Se resuelve denuncia por la realización de acciones publicitarias con bases de datos obtenidas en forma ilegítima.

RESOLUCION Nº		EXPEDIENTE Nº
69	2014	2013-2-10-0000132

Montevideo, 15 de mayo de 2014

VISTO:

La denuncia presentada por AA contra la empresa de telefonía BB (en adelante e indistintamente BB), en virtud "que realiza acciones publicitarias telefónicas con bases de datos obtenidos de manera ilegal".

RESULTANDO:

I) Que conferido traslado a BB informa que "la línea telefónica número 09XXXXXXX se encuentra asociada a la cuenta número 20XXXXX, bajo la titularidad de la empresa CC", a la cual solicita se le confiera vista, a lo que se accede en tres oportunidades, quedando en todos los casos truncada la notificación, en función de resultar incorrectos los domicilios aportados por BB.

II) Se solicitó a BB información y documentación detallada (fs. 52) previo informe jurídico, respecto de la cual sólo exhibió un Contrato de Agencia con DD, Sociedad de Hecho (sin sus Anexos).

CONSIDERANDO:

I) Que del objeto del Contrato agregado, surge que el Agente realizaba promociones, gestiones y obtenciones de pedidos por cuenta y orden de BB (cláusula 2.1) y que debía elaborar y mantener un registro de clientes potenciales con el nombre, documento de identidad, dirección, teléfono y "cualquier otra información que señale BB" y entregar en las instalaciones de esta última, luego de la firma de la solicitud de servicio "la totalidad de los documentos originales diligenciados junto con fotocopias de los documentos de identidad y aquellos que acrediten la representación legal en caso de tratarse de personas morales" (cláusula 6.5).

II) Que asimismo, BB exigía al Agente registrar sus actividades (registros de clientes, solicitudes de servicio, modificaciones) mediante pautas específicas, dejando expresa constancia en el Contrato, que dichos registros serán propiedad de BB y deberán estar a su disposición hasta tres años después de la terminación del Contrato de Agencia (cláusula 6.9)

III) Que de las disposiciones relacionadas y del Contrato, se desprende que la información personal utilizada por el Agente para su actividad es propiedad de la denunciada y su tratamiento se realizaba por su cuenta y orden. Por tanto cabe concluir que BB es responsable en sede de protección de datos conforme lo dispuesto en los artículos 4° literales H) y K) y 12 de la LPDP), siendo el Agente el encargado de tratamiento.

IV) Que por otra parte, BB no probó contar con el consentimiento del denunciante para utilizar su número de teléfono celular, o su origen de fuente pública, de acuerdo con lo dispuesto en los artículos 9° y 21 de la Ley N° 18.331, lo que además de ser su obligación, le fuera expresamente solicitado a fs. 52 de los presentes.

V) Que de las manifestaciones del denunciante respecto a que “El supervisor también rehusó darme el nombre de la empresa que realizaba este servicio y me cortó el teléfono ante la pregunta”, que no fueran objeto de controversia por la denunciada, se aprecia el incumplimiento del deber de informar dispuesto en el artículo 13 de la Ley N° 18.331.

VI) Que en relación a que los Agentes son considerados como proveedores de servicios e ingresan en la base de nombre proveedores, se advierten inconsistencias registrales, ya que los datos declarados no coinciden con la totalidad de la información que BB posee sobre sus agentes, según surge del Contrato agregado.

VII) Que en definitiva, la denunciada vulneró los artículos 9°, 13, 21 y 29 de la Ley N° 18.331.

VIII) Que ya ha sido apercibida por esta Unidad mediante Resolución N° 18 de 17 de Junio de 2009, recaída en Expediente N° 007/2009.

ATENTO:

A lo expuesto y a lo previsto en las normas aplicables,

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Sancionar con multa de 20.000 UI (veinte mil Unidades Indexadas) a BB por vulnerar los artículos 9°, 13, 21 y 29 de la Ley N° 18.331.
2. Intimar a BB a que adecúe su registro de proveedores a los datos que efectivamente trata, en plazo de 30 días corridos, bajo apercibimiento.
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 78, de 12 de junio de 2014.

Se resuelve denuncia por publicación de datos personales en un sitio web sin consentimiento del titular.

RESOLUCION Nº		EXPEDIENTE Nº
78	2014	2014-2-10-0000011

Montevideo, 12 de junio de 2014

VISTO:

La denuncia presentada por AA contra BB (en adelante BB), por publicar datos personales en la web sin su consentimiento.

RESULTANDO:

Que al evacuar el traslado, BB manifestó que en ningún momento otorgó acceso público a los referidos datos y que debido a un descuido interno de la empresa tercerizada (CC), una base de acceso restringido y de uso exclusivamente institucional e interno, quedó expuesta.

CONSIDERANDO:

I) Que BB es responsable del tratamiento de los datos del denunciante, conforme con lo dispuesto en los artículos 4 literales H) y K) y 12 de la Ley N° 18.331, siendo la empresa tercerizada (CC) el encargado de tratamiento.

II) Que la publicación de los datos del denunciante en la web, se enmarca en la definición legal de comunicación de datos personales dada por la citada norma, ya que se trata de una "revelación de datos realizada a una persona distinta del titular de datos".

III) Que resulta notoria la falta de consentimiento del titular para que sus datos, no contemplados en el artículo 9 literal c), sean publicados en la web, desvirtuando -además- la finalidad para la cual entregó la información.

IV) Que luego de haber sido intimada, BB presentó a inscribir sus bases de datos, advirtiéndose aún la falta de registro de la base de datos continente de la información que originó esta denuncia.

V) Que en definitiva, la denunciada incumplió en su calidad de responsable de tratamiento, los artículos 8, 9, 17 y 29 de la Ley N° 18.331, sin perjuicio de mostrar en todo momento una actitud colaborativa ante esta Unidad.

ATENTO:

A lo expuesto y a lo previsto en las normas aplicables,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Observar a BB, por incumplir lo dispuesto en los artículos 8, 9, 17 y 29 de la Ley N° 18.331.
2. Exhortar el registro de la base de dates continente de la información que generó la denuncia de obrados.
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 79, de 12 de junio de 2014.

Se resuelve denuncia sobre videovigilancia en el lugar del trabajo en el marco de la actividad sindical.

RESOLUCION Nº		EXPEDIENTE Nº
79	2014	2013-2-10-0000570

Montevideo, 12 de junio de 2014

VISTO:

La denuncia presentada por AA y BB, contra CC por considerar que son video vigilados en su lugar de trabajo desde que se han afiliado al sindicato de Artes Gráficas.

RESULTANDO:

I) Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista a las partes.

II) Que los denunciantes alegan que a partir de su afiliación sindical, se inicia una represión que incluye el seguimiento y el control de todos sus movimientos y de sus diálogos, a través de la instalación de un sistema de videovigilancia.

III) Que indican también que la base no está registrada y no cuentan con carteles de advertencia a la vista, así como nunca se les informó sobre su puesta en funcionamiento.

IV) Que la empresa manifiesta que ha dado aviso al personal y garantizado el derecho de acceso, aunque en el caso de la Sra. AA creen que hay abuso de derecho por la frecuencia en que el mismo ha sido ejercido. Se adjunta como prueba copia del recibo de entrega de un CD con datos personales, pero no presenta prueba (fotos u otra documentación) que indique la ubicación de las cámaras ni de los adhesivos de aviso.

V) Que también indican que el tiempo de conservación de las imágenes y micrófonos es de 24 horas, pero que realizan un respaldo en CD únicamente de “eventos puntuales y relevantes para ser utilizados como medios de prueba” y que estos datos “están a disposición de los titulares”.

CONSIDERANDO:

I) Que se está 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 se debe realizar un balance entre el derecho de la empresa a proteger sus bienes e instalaciones, y el derecho a la intimidad y a la protección de datos personales de los trabajadores, a la luz de los principios que inspiran la Ley, sobre todo los de consentimiento, finalidad y proporcionalidad (art. 5° parte final).

III) Que la utilización del sistema debe ser analizado en el marco del principio de proporcionalidad, considerando que ciertos lugares no pueden ser video vigilados (vestuarios, comedores, cocinas y baños), así como en el caso tampoco esa vigilancia debería llegar a ciertos lugares que no están dentro de la empresa, como por ejemplo el espacio frente a la reja de ingreso y la calle.

IV) Que en principio, siempre que los trabajadores sean informados debidamente y se consideren los límites, es legítimo instalar cámaras para controlar la actividad e instalaciones dentro de la empresa sin solicitar el consentimiento expreso de los trabajadores, (art. 9° Numeral D), teniendo en cuenta la proporcionalidad entre la finalidad y el tratamiento, sobre todo respecto a la ubicación, el alcance de la recopilación, para qué son utilizados los datos y la forma en que se informa a los trabajadores (arts. 6°, 7°, 8°, 9°, 12 y 13 de la LPDP.)

V) Que todas las apreciaciones acerca de los límites de la videovigilancia en el ámbito laboral se extraen tanto de la Ley N° 18.331 y su decreto reglamentario, explicitadas en el Dictamen N° 10/10 de la URCDP, así como del "Repertorio de recomendaciones prácticas de la OIT", adoptado en la reunión de expertos en Ginebra en 1996, sobre la protección de la vida privada de los trabajadores.

VI) Que el art. 4° E) de la Ley citada establece que ciertos datos son sensibles, y entre ellos los relativos a la afiliación sindical, por lo cual gozan de una regulación especial (art. 18), lo que debe ser tenido en cuenta por la empresa.

VII) Que además la empresa indica que realiza un respaldo en CD, por lo cual cabe inferir la existencia de una base de datos que contiene imágenes y audios, que debe ser inscripta en el registro (arts. 6°, 28 y 29 de la ley, arts. 15 a 20 del decreto N° 414/009.

VIII) Que con fecha el 21 de enero de 2014 se inició el proceso de inscripción de sus bases de clientes, empleados y videovigilancia.

IX) Que en el caso se aprecia la configuración de dos infracciones en relación a los artículos 13 y 6° de la citada ley (derecho de información y principio de legalidad).

X) Que por otra parte respecto al uso de la videovigilancia el mismo debe ser proporcionado y de acuerdo con los principios de la protección de datos.

XI) Que en cuanto al abuso de derecho de la denunciante que se esgrime por parte de la empresa, se tiene presente que el derecho de acceso puede ejercerse en forma gratuita a intervalos de 6 meses, salvo interés legítimo que debe acreditarse.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas y en la resolución N° 320/2011,

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Sancionar con UI 3.001 (Unidades Indexadas tres mil una) a CC.
2. Hacer saber a la denunciante acerca del plazo de seis meses previstos en el art. 14 de la Ley 18.331.
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 82, de 12 de junio de 2014.

Se resuelve denuncia por incumplimiento del derecho de supresión regulado en el artículo 15 de la Ley Nº 18.331.

RESOLUCION Nº		EXPEDIENTE Nº
82	2014	2012-2-10-0000790

Montevideo, 12 de junio de 2014

VISTO:

Las actuaciones cumplidas en el expediente N° 2012-02-10-0000790, de denuncia presentada por AA contra BB, por no dar de baja a su hijo del sistema de socios y seguir debitando de su tarjeta de crédito CC, a pesar de los diversos reclamos realizados.

RESULTANDO:

I) Que se otorga vista a los involucrados y CC se presenta aduciendo que no tienen responsabilidad alguna ya que hubo migración de datos y cambios en el sistema, indicando que es BB el que carga mal los datos.

II) Que se resuelve inspeccionar a este último y se constata que no se adoptan medidas de seguridad adecuadas para proteger los datos personales, en especial respecto de los datos de salud (fichas médicas de socios), por lo cual a tales efectos se les proporciona un documento de Buenas Prácticas de Seguridad para que se adopten alguna de ellas.

III) Que también se le intima a inscribir las bases de datos.

CONSIDERANDO:

I) Que la Unidad Reguladora, en tanto órgano de control en la materia, posee potestades legales tendientes a controlar la observancia del régimen normativo de su competencia.

II) Que el art. 10 de la Ley N° 18.331 indica que el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales.

III) Que BB es responsable de los riesgos que implica tratar datos sin medidas de

seguridad y de evitar errores como el que se ha denunciado, así como también es responsable de garantizar el ejercicio de los derechos de los titulares de los datos en tiempo y forma (art. 15).

IV) Que finalmente respecto a la obligación de inscripción, BB no tiene a la fecha sus bases inscriptas por ende está incumpliendo con lo establecido en el art. 6° de la Ley (Principio de Legalidad).

V) Que respecto a CC, ésta debe ser considerada un encargado de tratamiento de acuerdo a lo establecido en el art. 4° Literal H.

ATENTO:

A lo expuesto y lo dispuesto por los arts. 6°, 7°,10, 12, 15, 28, 29, 34 y 35 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. Sancionar con apercibimiento a BB por vulnerar los arts. 6°, 7°,10 y 15 de la Ley N° 18.331.
2. Otorgar un plazo de 30 días corridos a efectos de la inscripción de sus bases de datos considerando la posibilidad de aplicar una sanción mayor vencido el mismo.
3. Notifíquese, publíquese y posteriormente archívese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 83, de 12 de junio de 2014.

Se resuelve denuncia por violación a los principios de consentimiento, finalidad y otras disposiciones de la Ley Nº 18.331.

RESOLUCION Nº		EXPEDIENTE Nº
83	2014	2014-2-10-0000001

Montevideo, 12 de junio de 2014

VISTO:

La denuncia presentada por AA contra BB, en razón de una llamada recibida para ofrecer “el servicio” a su hija de 8 años que posee serios problemas de salud.

RESULTANDO:

Que al evacuar el traslado, BB manifiesta que desde el mes de diciembre incorporó un servicio de call center para ofrecer los distintos servicios de la firma y que “el teléfono móvil de la niña CC surgió por algún familiar o amigo allegado a la familia que utilizó nuestros servicios y lo dejó como referencia”.

CONSIDERANDO:

I) Que BB es responsable del tratamiento de los datos de la menor, conforme lo dispuesto en los artículos 4 literales H) y K) y 12 de la LPDP), siendo el call center encargado de tratamiento.

II) Que no resiste análisis que un menor de edad sea puesto como referencia comercial. Sin perjuicio, en caso de haber sucedido, ello no habilitaba a BB a utilizar dichos datos para enviar promociones comerciales, por desvirtuar la finalidad para la cual esa información le fue facilitada.

III) Que por otra parte, al tenor de las disposiciones del artículo 21 de la LPDP, los datos personales podrán ser tratados para ofrecer promociones comerciales, siempre que se encuentren en fuentes públicas de información o que sus titulares lo hubiesen consentido o facilitado.

IV) En el caso en estudio, ni los datos fueron consentidos por el titular conforme lo antes referido, ni se encontraban en fuente pública por tratarse de una menor de edad, lo que confirma la utilización de datos personales sin consentimiento del titular.

V) En definitiva, surge de obrados que la denunciada en su calidad de responsable de tratamiento vulneró los artículos 8, 9, 21 y 29 de la Ley N° 18.331.

ATENTO:

A lo expuesto y a lo previsto en las normas aplicables,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Apercibir a BB por vulnerar lo dispuesto en los artículos 8, 9, 21 y 29 de la Ley N° 18.331.
2. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 109, de 11 de setiembre de 2014.

Se resuelve denuncia por envío de tarjeta de crédito sin consentimiento.

RESOLUCIÓN Nº		EXPEDIENTE Nº
109	2014	2014-2-10-0000208

Montevideo, 11 de setiembre de 2014

VISTO:

La denuncia presentada por el Sr. AA contra BB y CC por el envío de una tarjeta de crédito sin su consentimiento.

RESULTANDO:

I) Que el denunciante ha recibido una tarjeta de crédito de BB con sus datos personales, los que fueron comunicados por la empresa CC sin su previo consentimiento, (artículo 17 de la Ley N° 18.331).

II) Que se solicitó la acreditación del consentimiento del denunciante para la comunicación de sus datos entre CC y BB, lo que no fue acreditado.

CONSIDERANDO:

I) Que la falta del consentimiento no está comprendida en las excepciones de los artículos 9° y 17 de la citada Ley.

II) Que la empresa CC contravino el principio de finalidad (artículo 8° de la Ley), utilizando los datos del denunciante para finalidades diferentes a aquéllas que motivaron su recolección sin su consentimiento.

ATENTO:

A lo expuesto, y a lo previsto en las normas vigentes de protección de datos,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Sancionar a CC con multa de 12.001 UI (doce mil una Unidades Indexadas) por no haberse ajustado al principio de previo consentimiento informado y al principio de finalidad, (artículos 8°, 9°, 17 y 35 de la Ley N° 18.331).
2. Sancionar a BB con multa de 12.001 UI (doce mil una Unidades Indexadas) por ser responsable solidario de CC, al quedar sujeto a las mismas obligaciones legales y reglamentarias que el emisor, de acuerdo con lo establecido en los artículos 17 y 35 de la Ley N° 18.331.
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Resolución Nº 127, de 29 de octubre de 2014.

Se resuelve petición relativa a la eliminación de datos de un sitio web.

RESOLUCIÓN Nº		EXPEDIENTE Nº
127	2014	2014-2-10-0000325

Montevideo, 29 de octubre de 2014

VISTO:

La petición formulada por AA para que se interceda ante BB a efectos de que determinada información personal que la afecta, no sea difundida en el sitio web.

RESULTANDO:

Que se han llevado adelante las actuaciones correspondientes y se comprenden las razones que se esgrimen respecto a las obligaciones de transparencia que alcanzan a todo organismo público.

CONSIDERANDO:

I) Que este Consejo Ejecutivo tiene potestades y cometidos específicos en materia de protección de datos personales según lo establecido en la Ley de N° 18.331

II) Que no obstante las obligaciones de transparencia, la Ley N° 18.331, art. 1°, consagra a la protección de datos personales como un derecho humano y se establece que la Unidad es el organismo encargado de velar por su respeto y garantías.

III) Que en razón de ello, se estima que deben aplicarse alguna de las técnicas comprendidas en la Resolución N° 1040/2012 del 20 de diciembre de 2012, basada en el informe técnico del CERT-uy, cuyo contenido se considera parte de esta resolución.

ATENTO:

A lo expuesto y a lo previsto en las normas aplicables,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Hacer saber a BB que corresponde considere la aplicación de alguna de las técnicas comprendidas en la Resolución N° 1040/2012, a la información objeto de la petición, a efectos de garantizar los derechos consagrados en la Ley N°18.331.
2. Notifíquese conjuntamente con la resolución antes mencionada, publíquese y oportunamente archívese.

Firmado:
Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Resolución Nº 130, de 29 de octubre de 2014.

Se resuelve sancionar a una empresa por incumplimiento de la intimación de inscripción de base de datos.

RESOLUCIÓN Nº		EXPEDIENTE Nº
130	2014	2014-2-10-0000067

Montevideo, 29 de octubre de 2014

VISTO:

La intimación formulada por esta Unidad para la inscripción o actualización de la base de datos de AA, otorgando a tales efectos un plazo de 30 días.

RESULTANDO:

Que transcurrido dicho plazo la empresa no se presenta a regularizar su situación.

CONSIDERANDO:

I) Que este Consejo Ejecutivo tiene potestades sancionatorias según lo indicado en el artículo 35 de la Ley N° 18.331 en su redacción dada por la Ley N° 18.719.

II) Que en el expediente resultan suficientemente explicitadas las circunstancias de hecho y de derecho que llevan a esta resolución.

ATENTO:

A lo expuesto e informado y a lo previsto en las normas aplicables,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Sancionar a AA con apercibimiento por vulnerar el art. 6° de la Ley N° 18.331 y los arts. 15 a 20 del decreto reglamentario N°414/009.
2. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Resolución Nº 141, de 19 de noviembre de 2014.

Se resuelve observar a una empresa por vulnerar el deber de información y los derechos de acceso y supresión.

RESOLUCIÓN Nº		EXPEDIENTE Nº
141	2014	2014-2-10-0000227

Montevideo, 19 de noviembre de 2014

VISTO:

La denuncia formulada por AA contra BB, por no suprimir sus datos personales de la base y continuar enviando publicidad.

RESULTANDO:

I) Que el denunciante presenta copia del correo enviado a la empresa con fecha 25 de abril de 2014, donde solicita que sus datos sean suprimidos de la base, así como documentación que prueba que continúa recibiendo publicidad a pesar de la mencionada solicitud (recibe con fechas 19 y 26 de mayo de 2014).

II) Que en ocasión de la solicitud se le responde que ya han sido eliminados sus datos, sin embargo, en las aclaraciones que se presentan ante la Unidad se indica expresamente que la cuenta fue desactivada recién con fecha 3 de junio de 2014, aduciendo que es posible que la cuenta se haya activado automáticamente en forma posterior a su solicitud en virtud de que el denunciante haya utilizado juegos o aplicaciones del sitio.

III) Que se agregan datos sobre las fechas en que se han utilizado los juegos, pero éstas son anteriores a la solicitud enviada por el denunciante, lo cual descarta la posibilidad de que su cuenta se activara de esa forma.

CONSIDERANDO:

I) Que el Consejo Ejecutivo de la URCDP tiene potestades y cometidos específicos en materia de protección de datos personales según lo establecido en el Ley de N° 18.331

II) Que el art. 4 Literal C) de la Ley N° 18.331 establece que el “consentimiento del titular es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne”.

III) Que BB afirma que ha enviado publicidad al denunciante, porque éste se ha suscripto al sistema y ha consentido utilizar los servicios, asumiendo lo informado en la Política de Privacidad existente en el sitio.

IV) Que revisada la Política de Privacidad del sitio cabe considerar que la misma no es fácilmente accesible para los usuarios, que no informa acerca de la base de datos, ni sobre la identidad y domicilio del responsable, ni de la posibilidad del titular de ejercer sus derechos, así coma tampoco advierte en forma clara y directa, que si se utilizan los juegos la cuenta se vuelve a activar, aunque ya hayan sido eliminados los datos asociados a la cuenta de correo electrónico. Por ende, el denunciante no ha sido debidamente informado, tal como se exige en

el art. 13 de la Ley.

V) Que BB ha procedido a darle de baja al denunciante pero lo ha hecho fuera del plazo previsto en la norma (arts. 14 y 15 de la Ley 18.331).

ATENTO:

A lo expuesto y a lo previsto en las normas aplicables,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Observar a BB por vulnerar los artículos 13, 14 y 15 de la Ley N° 18.331.
2. Intimar a BB a que en un plazo de 30 días adecue la Política de Privacidad de su sitio web, según lo establecido en el art. 13 de la Ley N° 18.331.
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Resolución Nº 142, de 19 de noviembre de 2014.

Se resuelve aplicar una sanción por comunicación de datos sin consentimiento.

RESOLUCIÓN Nº		EXPEDIENTE Nº
142	2014	2014-2-10-0000231

Montevideo, 19 de noviembre de 2014

VISTO:

La denuncia formulada por AA contra la Intendencia de Montevideo, por brindar acceso en forma indebida a sus datos personales, en el marco de una denuncia que realizó ante el Buzón BB.

RESULTANDO:

I) Que la denunciante aduce que se han comunicado sus datos personales al funcionario que ella misma ha denunciado por malos tratos y que con dicha información (incluido el celular y su domicilio), éste llamó a su casa para amenazarla.

II) Que asimismo, adjunta audio del programa de radio “bb “, cuyo texto y constatación notarial lucen agregados al expediente.

III) Que se le otorga vista a la Intendencia que expresa que no existió violación a la Ley N° 18.331, no obstante ello dispuso la instrucción de una investigación administrativa según Resolución N° 379/14/5000 de 8 de mayo de 2014, dictada por la Dirección General del Departamento de Gestión Humana y Recursos Materiales.

CONSIDERANDO:

I) Que el Consejo Ejecutivo de la URCDP tiene potestades y cometidos específicos en materia de protección de datos personales según lo establecido en el Ley de N° 18.331.

II) Que el art. 4 de la Ley establece que el consentimiento del titular es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consiente el tratamiento de datos personales. Asimismo define una base de datos como todo conjunto organizado de datos, independiente de su soporte.

III) Que surge del audio que cuando se hace contacto con el buzón ciudadano se piden datos personales, nombre completo, cédula de identidad, dirección, teléfono y e-mail, y dependiendo del contenido de la queja se envían a la dependencia correspondiente para trasladarle la respuesta a la persona denunciante.

IV) Que la base de datos que se forma a partir de estos formularios llenados por los interesados, no se encuentra inscripta en el Registro de la URCDP, en cumplimiento de lo dispuesto por el art. 6° de la Ley N° 18.331.

V) Que por otra parte, ingresado al sitio de la comuna se constata que, tanto durante el llenado del formulario del Buzón así como al finalizar la recolección de los datos, la Intendencia de Montevideo no informa a los usuarios acerca de la existencia de la base de datos, del responsable, la finalidad y el ejercicio de su derechos, tal como se establece en el art. 13 de la Ley N° 18.331.

VI) Que el art. 11 de la Ley establece que, aquellas personas físicas o jurídicas que obtuvieron legítimamente información proveniente de una base de datos, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros.

VII) Que en tanto el art. 7°. de la Ley establece que la recolección de datos no podía hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones de la Ley, por lo cual en el caso, el hecho de que la denunciante llene dicho formulario no significa de modo alguno que haya prestado su consentimiento para que otras personas (y mucho menos el denunciado), accedan a sus datos personales.

VIII) Que tampoco aplican al caso las excepciones previstas en la Ley, pues no se comunican los datos para cumplir con las funciones propias de los poderes del Estado, así como tampoco existe una obligación legal que habilite a dicho tratamiento.

IX) Que en consecuencia y en lo que atañe a los cometidos de la URCDP, se considera que ha existido una vulneración de la Ley N° 18.331, en diversos aspectos.

ATENTO:

A lo expuesto y a lo previsto en las normas aplicables,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Aplicar una sanción de apercibimiento a la Intendencia de Montevideo.

2. Indicar a la referida Intendencia que corresponde adecue la información disponible en su sitio respecto al Buzón, e intimarle proceda a la inscripción de la base de datos (Arts. 6° y 13 de la Ley N° 18.331).
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Resolución Nº 159, de 03 de diciembre de 2014.

Se resuelve denuncia por la cual se utilizó una etiqueta con datos personales en un sobre cerrado.

RESOLUCIÓN Nº		EXPEDIENTE Nº
159	2014	2014-2-10-0000270

Montevideo, 03 de diciembre de 2014

VISTO:
La denuncia presentada por el Sr. AA contra BB de CC por adherir en el exterior del sobre que contenía el Testimonio de una partida de estado civil solicitada vía web, una etiqueta conteniendo todos los datos personales del denunciante.

RESULTANDO:

I) Que conferido traslado la BB expresa que resulta imposible que vulnere lo dispuesto por la Ley 18.331, por lo previsto en el artículo 2 literal C ya que las bases de datos que maneja fueron creadas y reguladas por la Ley 1.430.

II) Que en el Registro de Bases de Datos que lleva esta Unidad no figuran bases de datos inscriptas a nombre de la BB ni a nombre de CC.

CONSIDERANDO:

I) Que el Consejo Ejecutivo de la URCDP tiene potestades y cometidos específicos en la materia de protección de datos personales según lo establecido en la Ley N° 18.331.

II) Que el art. 6° de la Ley N° 18.331 establece que la formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la Ley y las reglamentaciones que se dicten en consecuencia.

III) Que en dicho marco y en función de los hechos resultantes de la denuncia, se considera oportuno precisar que BB no debe inscribir los registros de estado civil propiamente dichos, pero sí respetar los principios contenidos en la Ley N° 18.331. Por lo tanto, no corresponde se expongan datos de un solicitante de testimonios de partidas que requieran consentimiento, en el exterior de un sobre de correo postal, reduciendo al mínimo los datos a incluir en la etiqueta adherida al sobre y adoptarse medidas para asegurar dichos datos.

ATENTO:

A lo expuesto, a lo previsto en las normas vigentes en la materia,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

Hacer saber a BB de CC que corresponde:

1. Atienda los principios rectores en materia de Protección de Datos Personales, velando por los datos de los solicitantes y reduciendo al mínimo los datos a incluir en la etiqueta adherida al sobre para su envío postal.
2. Inscriba sus bases de datos (funcionarios, proveedores, videovigilancia, etc)
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

DICTÁMENES

Dictamen Nº 1 de 5 de febrero de 2014

Se dictamina sobre el alcance de las modificaciones incorporadas a la Ley Nº 18.331 a través del artículo 9º Bis.

DICTAMEN N°		ACTA N°
01	2014	01/2014

Montevideo, 05 de febrero de 2014

VISTO:

Las modificaciones introducidas por la Ley N° 18.996, de 7 de noviembre de 2012, al agregar el artículo 9 bis a la Ley N° 18.331, de 11 de agosto de 2008.

RESULTANDO:

I) Que el artículo 9 bis de la Ley N° 18.331, establece que se consideran como públicas o accesibles al público, las siguientes fuentes o documentos:

A) El Diario Oficial y las publicaciones oficiales, cualquiera sea su soporte de registro o canal de comunicación.

B) Las publicaciones en medios masivos de comunicación, entendiendo por tales los provenientes de la prensa, cualquiera sea el soporte en el que figuren o el canal a través del cual se practique la comunicación.

C) Las guías, anuarios, directorios y similares en los que figuren nombres y domicilios, u otros datos personales que hayan sido incluidos con el consentimiento del titular.

D) Todo otro registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos puedan ser consultados, difundidos o utilizados por parte de terceros. En caso contrario, se podrá hacer uso del registro o publicación mediante técnicas de disociación u ocultamiento de los datos personales.

II) Que dicha disposición refiere a datos que ya se encuentran en fuente pública relacionados a la identidad de su titular.

CONSIDERANDO:

I) La necesidad de interpretar el tratamiento de datos personales no vinculados a la identidad de su titular.

II) Que los datos personales que no requieren previo consentimiento informado deben estar contenidos en listados.

III) Que por dictamen N° 26/2013, esta Unidad ha entendido que la palabra “listados” al no haber sido definida expresamente por el legislador, debe ser entendida en su sentido natural y obvio, según el uso general; y que de acuerdo con La Real Academia Española, listado viene del participio listar, que significa formar o tener listas, enumeración, generalmente en forma de columna, de personas, cosas, cantidades, que se hace con determinado propósito.

IV) Que toda interpretación sistemática y contextual de la Ley N° 18.331, debe realizarse de acuerdo con los principios rectores. Esta posición fue sostenida tanto por la URCDP como

por la Unión Europea durante el trámite de adecuación, quedando plasmado así en la Decisión de Ejecución de la Comisión Europea de 21 de agosto de 2012, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales

ATENTO:

A lo expuesto, a lo previsto en las normas legales citadas y en el artículo 34 literales A) y B) de la Ley N° 18.331,

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Que el artículo 9 bis de la Ley refiere a datos que ya se encuentran en fuente pública relacionados a la identidad de su titular.
2. Que conforme lo dispuesto en el Dictamen N° 26/2013, los datos personales que no requieren previo consentimiento informado deben estar contenidos en “listados” al momento de su recolección.
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 2 de 13 de febrero de 2014.

Se dictamina sobre la publicación de resoluciones que imponen sanciones a funcionarios públicos en el marco de la transparencia activa.

DICTAMEN N°		EXPEDIENTE N°
2	2014	2012-2-10-0000937

Montevideo, 13 de febrero de 2014

VISTO:

La consulta realizada por la Unidad Reguladora de Servicios de Comunicaciones (URSEC), respecto a la procedencia de publicar sanciones aplicadas a funcionarios públicos en su sitio web, sin vulnerar las disposiciones de la Ley N° 18.331, de 11 de Agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data y su decreto reglamentario N° 414/009 de 31 de Agosto de 2009.

CONSIDERANDO:

I) Que de acuerdo con lo estipulado en el principio de finalidad, previsto en el artículo 8° de la Ley N° 18.331, los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles a aquellas que motivaron su obtención, debiendo ser eliminados una vez que hayan dejado de ser pertinentes a los fines para los cuales hubieren sido recolectados,

evitando una perpetuidad en la sanción aplicada y consecuentemente perjuicios tales como los derivados del derecho al olvido.

II) Que será el responsable del contenido del sitio web, quien decida qué información será publicada, y por cuánto tiempo permanecerán esos datos disponibles en Internet, así como la aplicación de posibles controles o filtros a efectos de evitar la indexación por diversos motores de búsqueda, respecto a las resoluciones que contengan información personal, evitando una prolongación indeterminada en el tiempo y el espacio lo que naturalmente podría producir perjuicios al titular de los datos en cuestión.

III) Que salvo que exista interés público en conocer la identidad de los involucrados, correspondería aplicar a las resoluciones que contengan información de carácter personal un procedimiento de disociación de los datos, tal como se establece en el art. 17 literal D) de la Ley N° 18.331.

ATENTO:

A lo expuesto por las disposiciones de la Ley N° 18.331, de 11 de Agosto de 2008 y en 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 DICTAMINA:

1. Señalar que la publicación de resoluciones que imponen sanciones a funcionarios públicos en el marco de las obligaciones de transparencia activa del organismo, no vulnera las disposiciones de la Ley N° 18.331, en tanto se hayan considerado los principios y excepciones previstas en la norma.
2. Salvo que exista interés público en conocer la identidad de los involucrados, caso en que deberá atenderse a lo detallado en los considerandos I y II, se recomienda aplicar a las resoluciones que contengan información personal un procedimiento de disociación de los datos, tal como se establece en el art. 17 inc. D) de la Ley N° 18.331.
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 3, de 13 de maro de 2014.

Se dictamina respecto a la consulta formulada por la Intendencia de Florida relativa a la posibilidad de brindar acceso a información de un determinado contribuyente.

DICTAMEN Nº		EXPEDIENTE Nº
03	2014	2014-2-10-000562

Montevideo, 13 de marzo de 2014

VISTO:

La consulta formulada por la Intendencia Departamental de Florida, respecto a brindar acceso a copia de la documentación que ha sido entregada por parte de determinado contribuyente, con el fin de realizar el trámite de empadronamiento de un vehículo.

RESULTANDO:

I) Que un Edil Departamental está solicitando tener acceso a esa documentación que incluye: carta de la casa vendedora (certificada), Certificado de Importación (cert. Industria), Inspección Técnica, Cédula de Identidad, Certificado de Residencia y si no es el propietario Carta Poder certificada.

II) Que el expediente fue remitido a la Unidad de Acceso a la Información Pública (UAIP), y a fojas 9 se indica que surge de la consulta que la temática de la misma corresponde a la Unidad Reguladora y de Control de Datos Personales.

CONSIDERANDO:

I) Que las intendencias son sujetos obligados por la Ley N° 18.381, que si bien establece la obligación de brindar acceso a la información que les es solicitada, también obliga a analizar y clasificar la información amparada por alguna de las excepciones, y en el caso el acceso contiene información confidencial, pues se trata de datos personales que requieren previo consentimiento informado según se establece el art. 10 Num. II de dicha Ley.

II) Que por otra parte, el art. 1° de la Ley N° 18.331 reconoce que el derecho a la protección de datos personales es inherente a la personalidad humana y está comprendido en el art. 72 de la Constitución Nacional, por ello, si bien es cierto que el pedido de informes realizado por un Edil Departamental se enmarca en lo establecido en el art. 284 de la misma, corresponde que se pondere el derecho humano y el sistema de protección especial que se sustenta en la propia Carta Magna.

III) Que por ello, a la hora de brindar acceso a información personal que por determinado motivo se encuentra en poder de un organismo público (en este caso la Intendencia de Florida)-; indefectiblemente debe realizarse un juicio de proporcionalidad, basado en la idoneidad, la necesidad y el equilibrio de derechos, y debe existir una justificación que muestre como imprescindible la utilización de esa información, por ejemplo para investigar un delito, evitar un peligro inminente o contribuir a determinada investigación judicial, y si este fuera el caso, la

información debería ser solicitada a través de la justicia.

IV) Que por otra parte, la Intendencia recoge esa información para brindar un servicio específico, o sea para determinada finalidad que debe ser respetada (art. 8° de la Ley N° 18.331).

V) Además, el artículo 9° c) de esta norma enumera una serie de datos personales que no requieren el previo consentimiento informado para su comunicación (nombre y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento), y en el caso, la información solicitada excede este listado e incluye otros datos o información que sí lo requiere.

VI) Que por otra parte el art. 17 de la misma, respecto a la comunicación de datos personales, exige la conjunción simultánea del interés legítimo del emisor y del destinatario de la comunicación, y el previo consentimiento del titular de los datos, salvo las excepciones establecidas, y en el caso, dado el tenor de la consulta, se entiende que no existe interés en el titular de los datos así como tampoco su consentimiento.

VII) Que finalmente, el Consejo Ejecutivo de la URCDP ya se ha expresado en forma negativa en cuanto a brindar la información personal de determinados beneficiarios de servicios del Estado en los Dictámenes N° 15 del 15 de setiembre de 2011 (consulta del Fondo de Solidaridad), N° 10 de 2012 (consulta formulada por la Intendencia de Rocha), y por último, en consulta similar formulada por la Unidad de Acceso a la Información Pública, en razón de la solicitud de acceso planteada ante la Intendencia de Montevideo, a través del Dictamen N° 12 de 7 de junio de 2012.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Comunicar a la Intendencia de Florida que sólo estaría legitimada para entregar al solicitante, información relacionada con el empadronamiento de vehículos en forma general y disociada de los titulares del trámite.
2. Notifíquese, publíquese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 4, de 3 de abril de 2014.

Se dictamina sobre la consulta formulada por el Colegio Médico del Uruguay sobre la legalidad de realizar una comunicación de datos al Fondo de Solidaridad

DICTAMEN Nº		EXPEDIENTE Nº
04	2014	2014-2-10-000097

Montevideo, 03 de abril de 2014

VISTO:

La consulta formulada por el Colegio Médico del Uruguay (CMU), respecto a la posibilidad de que el Fondo de Solidaridad le comunique el listado de los médicos en actividad, con el fin de actualizar la base de datos que se posee para cumplir con sus cometidos legales.

RESULTANDO:

I) Que el CMU es una persona pública no estatal creada por ley N° 18.591 de 18 de setiembre de 2009, que determina su competencia y cometidos.

II) Que solicita que el Fondo de Solidaridad le comunique los datos de los médicos que egresan, a efectos de actualizar el registro, considerando que el MSP comunica dicha información pero la base de datos no está debidamente depurada (de jubilados o fallecidos).

CONSIDERANDO:

I) Que la Ley N° 18.591 crea al CMU "como persona jurídica pública no estatal, con el cometido de garantizar al médico y a la comunidad, el ejercicio de la profesión dentro del marco deontológico establecido" y en el art 2º, establece la obligatoriedad de la inscripción en sus registros, pues para "ejercer la profesión de médico en el territorio nacional, se requerirá la vigencia de la inscripción en el registro de títulos del Colegio Médico del Uruguay".

II) Que no obstante ello, la obligación de mantener un registro actualizado es atribuida por la Ley al CMU que es quien formula la consulta, o sea no se trata de una obligación legal atribuida a quien va a realizar la comunicación de datos, que en el caso sería el Fondo de Solidaridad, por ello no aplicaría la hipótesis prevista en el art. 9 B) de la Ley N° 18.331.

III) Que en cambio, correspondería aplicar la excepción prevista en el art. 9 D), pues resulta de interés de los profesionales médicos, y a su vez constituye una obligación el estar inscriptos en dicho registro para poder ejercer como médico (art. 2 de la Ley N° 18.591).

IV) Que también el art. 17 de esta norma, referido a la comunicación específicamente, establece que los datos objeto de tratamiento podrán ser comunicados sin previo consentimiento, cuando así lo disponga una ley de interés general o en los supuestos del art. 9°, así como debe identificarse un interés legítimo, tanto de quien comunica los datos como del titular de los mismos, cuestión que en el caso se verifica.

V) Que por otra parte, aunque opere una comunicación de datos personales que involucra al Fondo de Solidaridad, -excepcionado de recabar el consentimiento como ya se

analizó-, también se trata de un intercambio de información que incluye datos personales, por ello debe considerarse lo previsto en los arts. 157 a 160 de la Ley N° 18. 719 de 27 de diciembre de 2010, sobre intercambio de información entre Entidades Públicas, estatales o no, así como su decreto reglamentario N° 178/013.

VI) Que respecto a la posibilidad de realizar intercambio con otras instituciones públicas estatales o no, ya sea BPS o Caja de Jubilaciones y Pensiones de Profesionales Universitarios, se considera factible y corresponde estar también a lo dispuesto en la normativa específica antes mencionada.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Informar al consultante que son aplicables el inciso D) del artículo 9° y el art. 17 de la Ley N° 18.331 que eximen al Fondo de Solidaridad de recabar el consentimiento informado de los titulares de los datos, a efectos de que los mismos sean comunicados al CMU.
2. Que no obstante ello, se recomienda estar a lo dispuesto por los arts. 156 a 160 de la Ley N° 18.719, que indica que se debe formalizar un acuerdo de intercambio de información entre Entidades Públicas, estatales o no, con las condiciones y requisitos ya mencionados.
3. Notifíquese, publíquese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 5, de 30 de abril de 2014.

Se dictamina sobre la consulta realizada por el Programa Salud.uy relativa a la legitimidad del tratamiento de datos de salud del componente Teleimagenología.

DICTAMEN Nº		EXPEDIENTE Nº
05	2014	2014-2-10-00000100

Montevideo, 30 de abril de 2014

VISTO:

La consulta formulada por el Director del Programa Salud.uy, Ing. Jorge Forcella, sobre la legitimidad del tratamiento de datos de salud, en el marco del Componente de Teleimagenología.

RESULTANDO:

I) Que lo proyectado incluye un Sistema de Información Radiológico, con una arquitectura que permite realizar consultas en forma remota por parte de los centros de salud o por médicos especialistas actuando individualmente.

II) Que también se ofrecerá una plataforma de alcance general (público y privado), para la complementación de servicios en el área, a nivel de todo el país.

III) Que las comunicaciones se realizarán sobre un canal seguro que es la RedUY, y mediante una red local aislada de forma lógica, así como las bases de datos residirán en servidores independientes y exclusivos para las tareas de imagenología.

IV) Que los datos que visualizan los técnicos y médicos serán: CI, nombres y apellidos, fecha de nacimiento y sexo, asociadas a las imágenes.

CONSIDERANDO:

I) Que se trata de una comunicación de datos personales en el entorno de los servicios de salud, por lo cual corresponde la aplicación de la Ley N° 18.331.

II) Que el Derecho a la Salud abarca el derecho de acceso a todos los servicios, facilidades, bienes, etc, disponibles para alcanzar el mejor nivel de salud posible, y en este sentido el sistema implica beneficios para los pacientes y usuarios, resultado del avance de la ciencia y la tecnología aplicados a la mejora de los servicios de salud.

III) Que el art. 17 de la Ley citada 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.

IV) Que además según el art. 4° los datos de salud son datos sensibles, y por ello ninguna persona puede ser obligada a proporcionarlos, si bien podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular (art. 18).

V) Que por ende el consentimiento del titular, enerva cualquier obstáculo y habilita el tratamiento de estos datos, pero al estar en presencia de un plan o proyecto que apunta a

mejorar los servicios de salud-, también median razones de interés general en el entendido de que el Estado debe garantizar el disfrute de toda una gama de facilidades, bienes, servicios y condiciones necesarios para alcanzar el más alto nivel posible de salud.

VI) Que en cuanto al mandato legal, hay que considerar la existencia de un abundante marco específico que refiere al sistema de salud, haciendo énfasis en la Ley N° 18.335 y su decreto reglamentario N° 274/010.

VII) Que si fuere necesario formalizar el intercambio de información entre entidades del ámbito público, será de aplicación la Ley Nº 18.719, de 27 de diciembre de 2010, que brinda garantías para las partes.

VIII) Que respecto a si es conveniente anonimizar la información personal mediante algún componente informático, se considera que ello no es necesario, pues identificar los estudios que se realicen redunda en la calidad de la información y beneficia a los pacientes en cuanto a la certeza de que ellos le pertenecen.

IX) Que en definitiva, considerando lo establecido en los arts. 9 B), 9 D), 17 y 18 de la Ley N° 18.331, así como lo expresado en los arts. 6°. 7°, 11 y 18 de la Ley N° 18.335, corresponde concluir que es legítima la recolección, el tratamiento y la comunicación de datos, descriptos en la consulta que se ha formulado.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que la recolección, comunicación y tratamiento de datos personales realizado en el escenario descripto en la consulta efectuada por el Director del Programa Salud.uy se adecua a la normativa de protección de datos personales.
2. Señalar que por tratarse de datos de salud, deberán observarse estrictamente los principios y demás obligaciones previstas en las normas mencionadas en la parte expositiva de este Dictamen, haciendo especial énfasis en la seguridad de la información.
3.- Notifíquese, publíquese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 7, de 8 de mayo de 2014.

Se dictamina sobre consulta realizada por Seguros Uruguay S.A (AIG) relativa a la legalidad de realizar transferencias internacionales de datos personales.

DICTAMEN Nº		EXPEDIENTE Nº
07	2014	2014-2-10-0000123

Montevideo, 8 de mayo de 2014

VISTO:

La consulta formulada por SEGUROS URUGUAY S.A. (AIG) sobre la viabilidad de obtener autorización para la transferencia internacional de datos personales entre la mencionada e International Business Machines Corporation (IBM) y se exprese sobre la redacción del contrato y los documentos presentados, en lo que se aplique a las empresas en el ámbito local.

RESULTANDO:

Que las transferencias internacionales se realizan a países que cuentan con normas de protección adecuadas y medios para asegurar su aplicación eficaz y también a aquellos que no cuentan con estas condiciones previa autorización de la Unidad.

CONSIDERANDO:

I) Que la legalidad respecto a las transferencias internacionales de datos, objeto de la consulta, se encuentra regulada en la Ley Nº 18.331.

II) Que la transferencia internacional de datos es realizada con IBM, cuya sede es en Nueva York, Estados Unidos, país que cuenta con el sistema de “Safe Harbor”, al igual que la empresa, cumpliendo con las garantías suficientes para la realización de esta, sin necesidad de autorización, de acuerdo con lo establecido en la Resolución de la Unidad Nº 17 de 12 de junio de 2009.

III) Que la relación existente entre ambas empresas se encuentra basada en un Contrato Marco de Servicios de Alojamiento (Hosting) Web y en la Declaración de Trabajo de IBM para Servicios i-Claims, Chartis Claims, Inc. que se plasma en el Acuerdo Local para la Declaración de Trabajo antes mencionada entre las dos empresas en Uruguay, los que se entiende están de acuerdo con la normativa aplicable.

IV) Que en dicho Acuerdo las partes se comprometen a incluir las disposiciones de la Ley Nº 18.331 en la cláusula de “Legislación de Privacidad”

V) Que las consideraciones anteriores se encuadran dentro de la Ley Nº 18.331 artículo 23, su decreto reglamentario Nº 414/009, artículos 34 y 35, la Resolución Nº 17 de 12 de junio de 2009 y el Dictamen Nº 8 de 19 de marzo de 2010.

ATENTO:

A lo expuesto, y a lo previsto en las normas, Resolución y Dictamen anteriormente citados,

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

Señalar que:

a) la transferencia internacional de datos entre las empresas AIG e IBM se encuentra dentro de lo previsto por la Ley Nº 18.331, su decreto reglamentario, la Resolución Nº 17 de 12 de junio de 2009 y el Dictamen Nº 8 de 19 de marzo de 2010 correspondientes a esta Unidad.

b) El contrato local entre las empresas mencionadas –en la redacción presentada ante la Unidad-, así como su documentación conexa, resultan acordes con la normativa citada en la parte expositiva de este dictamen.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 8, de 23 de julio de 2014.

Se dictamina sobre el tratamiento de datos personales en la nube.

DICTAMEN Nº		EXPEDIENTE Nº
08	2014	2014-2-10-0000233

Montevideo, 23 de julio de 2014

VISTO:

La consulta formulada por el Ing. Rafael Méndez de Integración AFAP sobre tratamiento de datos en la nube.

RESULTANDO:

I) Que Integración AFAP está en proceso de selección de un CRM y una de sus opciones es el software RightNow de la firma Oracle en modalidad SaaS, por tanto la aplicación y los datos contenidos en ella estarán en la nube de Oracle.

II) Que según el proveedor esa nube tiene varios Datacenter en distintas partes del mundo para asegurar la disponibilidad del servicio.

III) Que Integración AFAP tiene cerca de 200.000 afiliados, cuyos datos personales serán accedidos desde el CRM, y se almacenarán como mínimo: nombre, dirección, teléfono, sueldo, lugar de trabajo, fecha de nacimiento.

CONSIDERANDO:

I) Que la situación encuadra dentro del ámbito de aplicación definido por la Ley N° 18.331 (art. 3°) y en las hipótesis previstas en los Literales A y B del artículo 3° del Decreto N° 414/009, reglamentario de la Ley.

II) Que corresponde determinar si se está o no ante una transferencia de datos en el

sentido establecido en el art. 4° Literal H) de dicho Decreto.

III) Que en la consulta se indica que los datos “se subirán” a la nube, por lo cual habría transferencia ya que la base se encuentra en un servidor ubicado en el exterior del país aunque sea a modo de respaldo.

IV) Que es fundamental destacar que se está ante una transferencia internacional de datos, considerando especialmente en este sentido, la importancia que tiene que, tanto el servicio como los respaldos, se encuentren ubicados en países adecuados en materia de protección de datos personales.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que en la situación planteada en la consulta formulada por Integración AFAP en estos obrados existe transferencia internacional de datos en el sentido de lo establecido en la Ley 18.331 y su decreto reglamentario 414/009, en especial su art. 4° Literal H).
2. Hacer saber que en virtud de la legislación citada en el numeral anterior, tanto el servicio como los respaldos, deberán ubicarse en países adecuados en materia de protección de datos personales.
3. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 9, de 19 de agosto de 2014

Se dictamina sobre consulta de la UNASEV relativa a la creación del Sistema Nacional Unificado de Datos.

DICTAMEN Nº		EXPEDIENTE Nº
09	2014	2014-2-10-0000509

Montevideo, 19 de agosto de 2014

VISTO:

La solicitud de asesoramiento de la Unidad Nacional de Seguridad Vial (UNASEV) en relación con la implementación del Sistema Nacional Unificado de Datos, en base a sus competencias para la supervisión de los Registros referidos en el artículo 60 de la Ley N° 18.113, de 18 de abril de 2007.

CONSIDERANDO:

I) Que la Ley N° 18.113 crea como órgano desconcentrado del Poder Ejecutivo a la

Unidad Nacional de Seguridad Vial, para la regulación y el control de las actividades relativas al tránsito y la seguridad vial en todo el territorio nacional, así como para analizar las causas de los siniestros de tránsito y demás aspectos referidos a éstos, propiciando la utilización de las estadísticas para ser aplicadas a la elaboración o actualización de la normativa relativa al tránsito y la seguridad vial.

II) Que a los efectos de cumplir sus objetivos, la UNASEV ha resuelto crear un Sistema Nacional Unificado de Datos.

III) Que una interpretación contextual de la norma a la luz del objetivo central de regular y controlar las actividades relativas al tránsito y la seguridad vial en todo el territorio nacional, sumada a las competencias atribuidas, resulta suficiente para sostener que la UNASEV se encuentra habilitada para crear el referido Sistema Nacional Unificado de Datos.

IV) Que aplica al nuevo sistema de información aludido la Ley de Protección de Datos Personales y Acción de Habeas Data.

V) Que en relación con los datos sobre violencia, aún frente a la hipótesis de considerarse necesarios para el dictado de políticas públicas en la materia, deberá atenderse especialmente a la proporcionalidad, la confidencialidad y la reserva en todo tratamiento que se haga de esa información, para evitar la discriminación, la persecución y la estigmatización de los titulares de esos datos.

VI) Que el sistema unificado deberá ser inscripto ante el Registro de esta Unidad, así como también las bases que lo alimentan, salvo que sean creadas y reguladas por leyes especiales.

VII) Que los derechos de los titulares de los datos se ejercerán ante la UNASEV.

ATENTO:

A lo expuesto e informado, y lo previsto por los arts. 31 y 34 de la Ley Nt 18.331.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. La UNASEV posee competencias legales para crear el Sistema Nacional Unificado de Datos.
2. El sistema unificado deberá ser inscripto ante el Registro de esta Unidad así como también las bases que lo alimentan, salvo que sean creadas y reguladas por leyes especiales.
3. Los derechos de los titulares de los datos se ejercerán ante la UNASEV.
4. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 12, de 4 de setiembre de 2014.

Se dictamina sobre publicación de certificados de defunción en sitio web.

DICTAMEN Nº		EXPEDIENTE Nº
12	2014	2014-2-10-0000281

Montevideo, 04 de setiembre de 2014

VISTO:

La consulta presentada por el Ministerio de Salud Pública en relación con el certificado de defunción y el certificado de defunción resumido en cuanto a su publicación en la web.

CONSIDERANDO:

I) Que tanto el certificado de defunción como el certificado de defunción resumido contienen datos personales y datos personales sensibles (artículo 41 literales D) y E) de la Ley N° 18.331).

II) Que para ambos tipos de datos es necesario el consentimiento libre, previo, expreso, informado y documentado de su titular, agregándose como requisito para los datos sensibles estar por escrito.

III) Que el Ministerio de Salud Pública y el Instituto Nacional de Estadística están realizando un trabajo de colaboración para la publicación de los certificados de defunción y de nacido vivo en la página web. Dicha publicación podrá ser realizada si se tiene el consentimiento del titular del, dato, en el caso de las defunciones aquél de sus herederos, con la excepción prevista en el artículo 90 literal C) de la Ley N° 18.331 y si se disocian los datos.

IV) Que los certificados de defunción no están comprendidos dentro del concepto de fuente pública establecido en el artículo 91 bis, de la Ley, por lo que la entidad pública que podría proporcionarlos es la Dirección General del Registro de Estado Civil en su carácter de registro público y no el Ministerio de Salud Pública.

ATENTO:

A lo expuesto, y a lo previsto en la Ley N° 18.331, arts. 41 literales D) y E), 16 y 18 y al Decreto Nº 431/011, de 4 de diciembre de 2011 y normas concordantes,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Para la publicación de los certificados de defunción en la página web, el Ministerio de Salud Pública debe solicitar el consentimiento libre, previo, expreso, informado de los herederos del titular. En el caso de los datos sensibles se necesita además, que sea por escrito.
2. No se requerirá el consentimiento para su publicación si los datos están dentro de los enumerados en el artículo 9° literal C) de la Ley N° 18.331 o si están disociados.
3. No es de aplicación al certificado de defunción y al certificado de defunción resumido el artículo 9° bis de la Ley N° 18.331, por no estar comprendido dentro de sus enunciados.

Solo la Dirección General del Registro de Estado Civil es la que puede proporcionar estos certificados como fuente pública.

4. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 14, de 2 de octubre de 2014.

Se dictamina sobre consulta presentada por la Caja Notarial de Seguridad Social relativa a la adecuación de formularios diseñados por el organismo para utilizar servicios electrónicos.

DICTAMEN Nº		EXPEDIENTE Nº
14	2014	2014-2-10-0000337

Montevideo, 02 de octubre de 2014

VISTO:

La consulta presentada por la Caja Notarial de Seguridad Social.

RESULTANDO:

I) Que dicha institución ofrece servicios electrónicos a sus afiliados para el ejercicio de sus derechos y cumplimiento de sus obligaciones. A tales efectos, instrumentó formularios de solicitud de utilización de dichos servicios, que contienen, además, de una autorización expresa para realizar comunicaciones mediante la utilización de correo electrónico.

II) Que actualmente la Caja se encuentra abocada a una reingeniería que permitirá a los afiliados el acceso remoto a más servicios y datos que los originalmente instrumentados. Paralelamente, enfrenta un incremento de solicitudes de sus afiliados de envío de información por correo electrónico.

III) Que se consulta a esta Unidad sobre la suficiencia de los formularios ya utilizados o la pertinencia de requerir autorizaciones adicionales de sus afiliados.

CONSIDERANDO:

Que estudiados los formularios presentados denominados “Solicitud de utilización de servicios electrónicos Afiliados Empleados” y “Solicitud de utilización de servicios electrónicos Afiliados Escribanos”, se considera que sus previsiones son adecuadas.

ATENTO:

A lo expuesto e informado, y lo previsto por los artículos 31 y 34 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. Señalar que se consideran suficientes las previsiones contenidas en los formularios presentados por la Caja Notarial, denominados “Solicitud de utilización de servicios electrónicos Afiliados Empleados” y “Solicitud de utilización de servicios electrónicos Afiliados Escribanos”.
2. Notifíquese, publíquese y oportunamente archívese.

Firmado:
Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

INFORMES

Informe Nº 193, de 23 de setiembre de 2013

Se informa consulta relativa a la publicación de datos de sanciones a funcionarios públicos.

INFORME Nº		EXPEDIENTE Nº
193	2013	2012-2-10-0000937

Montevideo, 23 de setiembre de 2014

I. Contenido de la consulta en análisis

Con fecha 30 de noviembre de 2012 la Sra. Directora de la Unidad Reguladora de Servicios de Comunicaciones (URSEC) Lic. AA solicita formalmente a través de nota dirigida a la Unidad de Acceso a la Información Pública (UAIP) un pronunciamiento con carácter extensivo a la Unidad Reguladora y de Control de Datos Personales (URCDP), respecto a la procedencia de publicar sanciones aplicadas a funcionarios públicos, en el marco de su actuación y habiéndose otorgado las garantías correspondientes al procedimiento disciplinario.

Expresa adicionalmente la Lic. AA en la referenciada solicitud que para el caso de un pronunciamiento afirmativo respecto a la publicación de la información consultada, cuál sería el carácter y vigencia de su aplicabilidad en atención al otorgamiento de un tratamiento igualitario y no discriminatorio a todos los funcionarios que hayan sido pasibles de las mismas.

Advierte en la solicitud formulada que con fecha 31 de julio de 2012 el Directorio de la URSEC, a través de la Resolución N 102 Acta 019, clasificó como reservada entre otras, la información contenida en cualquier soporte, que constituya documento de trabajo interno y preparatorio de cualquier decisión administrativa. Sin perjuicio de lo cual destaca que no existe una definición sobre publicar o no las sanciones que resulten de un procedimiento sancionatorio a funcionarios públicos.

En definitiva, se requiere un pronunciamiento formal de la URCDP a efectos de fijar criterios a considerar ante una eventual publicación de las sanciones aplicadas a funcionarios de la URSEC en la página web del organismo, sin vulnerar el derecho a la protección de datos personales.

En forma preliminar al análisis encomendado, estimo oportuno señalar que en opinión de este informante no existen soluciones uniformes y globales que puedan abarcar la universalidad de hipótesis que eventualmente pueden plantearse en cada caso en concreto, ante el caso de dudas particulares y dada la universalidad de situaciones posibles será conveniente consultar nuevamente la opinión de uno o ambos Órganos de Control (UAIP o URCDP).

II. Sobre la reserva de resoluciones que disponen aplicación de sanciones

En cuanto a la posibilidad de clasificar con carácter de reservadas las resoluciones que imponen aplicación de sanciones a los funcionarios del Organismo, cuando su divulgación pueda poner en riesgo la dignidad humana de la persona sancionada, previa realización de la correspondiente prueba de daño, se ha pronunciado mediante Dictamen N° 11/2013, de fecha 13 de setiembre de 2013 la UAIP, competente en dicha materia en virtud de las disposiciones de la Ley N° 18.381 y decreto reglamentario. En plena concordancia con el pronunciamiento de la UAIP, durante el transcurso de un procedimiento Sumario Administrativo y hasta tanto el mismo no se encuentre firme, podría ser clasificado como información reservada por parte del Directorio de la URSEC, indicando expresamente el fundamento de dicha reserva.

Adicionalmente y según el Manual de Clasificación de la Información en Poder de los Sujetos Obligados por la Ley de Acceso a la Información Pública, realizado por la UAIP[1] : "nadie puede dudar que la vida y dignidad humanas, la seguridad y la salud de las personas, son derechos fundamentales cuya mejor garantía de preservación puede, en ciertos casos, depender del mantenimiento de determinadas informaciones al abrigo del escrutinio público".

En definitiva la declaración de reserva debería durar hasta tanto se resuelva definitivamente sobre el asunto, ya que una vez otorgadas las garantías y preservada la dignidad de la persona, debería brindarse acceso a la resolución que corresponda, en los términos que analizaremos más adelante de acuerdo a la Ley N° 18.331.

En este sentido es importante tener en consideración que en atención al Principio de Divisibilidad de la Información, y en cuanto las circunstancias lo ameriten, también podrá clasificarse sólo una parte de esa información como reservada o confidencial de acuerdo con el art. 10 in fine de la Ley N° 18.381.

III. Principio del previo consentimiento informado

En atención al Principio del previo consentimiento informado, el que constituye uno de los pilares esenciales en materia de protección de datos personales y es recogido a texto expreso

1- A efectos de establecer pautas la Unidad de Acceso a la Información (UAIP) de acuerdo al Acta N°9/2009, aprobó un manual denominado "Manual de Clasificación de Información en Poder de los Sujetos Obligados por la Ley de Acceso a la Información Pública". Al respecto debe consultarse a esta Unidad. Se agrega en dicho manual, que "este juicio de valor (prueba del daño) lo debe realizar el jerarca, para de esa forma motivar y fundamentar legalmente el acto de clasificación" y se aclara también que "puede resultar aconsejable el empleo de esta vía para no dejar librado a la confidencialidad o al secreto algunas situaciones donde no existe norma de rango legal (ej. el secreto de la investigación y sumario administrativo) o en aquellas situaciones en que existen interpretaciones opinables (ej. la extensión exacta del secreto bancario en nuestro derecho). La ventaja de contar con una declaración expresa de reserva se traduce, en tales casos, en seguridad jurídica".

en el artículo N° 9 de la Ley N° 18.331[2] (en lo sucesivo LPDP), el tratamiento de datos personales será lícito cuando el titular del dato hubiere prestado su consentimiento libre, previo, expreso e informado, a tales efectos.

Sin perjuicio de lo expuesto y en atención al precitado artículo de la LPDP, existen determinados datos personales que no requieren para su tratamiento el previo consentimiento del titular. En el caso de personas físicas: nombres y apellidos, documento de identidad, domicilio, nacionalidad y fecha de nacimiento y respecto a las personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de los responsables.

Adicionalmente, la Ley N° 18.331 establece expresamente que existen otros datos que tampoco requieren previo consentimiento informado: a) los datos que provengan de fuentes públicas de información, b) los datos que figuran en registros públicos por disposiciones legales y c) los que figuren en publicaciones de medios masivos de comunicación.

Por su parte, el literal b) del artículo 9° establece que no será necesario recabar el previo consentimiento informado, cuando se está ante el "ejercicio de funciones propias de los Poderes del Estado", o la recolección de datos se efectúa "en virtud de una obligación legal". En este sentido, tomando en consideración los cometidos legales de la URSEC y la relación funcional de los sujetos que en dicha repartición prestan labores, cabe inferir que no será necesario recabar el consentimiento de los funcionarios a efectos de cumplir con los cometidos de la Administración, entre los cuales naturalmente se encuentra el de contralor y eventualmente el de imponer una sanción a un funcionario cuando fuere procedente y mediante el otorgamiento de las garantías legales que al caso correspondan.

Lo expuesto, no significa que deba publicarse el contenido completo de las resoluciones del organismo sin recabar el consentimiento y sin preservar el derecho a la protección de datos personales, pues ese no necesariamente configura el interés del titular del dato a la hora de brindar su información a un organismo público.

Es trascendente destacar que en aquellos casos en donde lo público y lo privado se entrecruzan, deben aplicarse los principios que rigen la Ley N° 18.331. En especial es relevante valorar la finalidad y la proporcionalidad de los datos utilizados, como verdaderos ejes o pilares fundamentales del derecho a la privacidad tutelado, el que es expresamente reconocido en nuestro sistema jurídico como un derecho humano fundamental[3].

---

2. Véase art. 9 de la Ley N° 18.331 publicada el día 18 de agosto de 2008, Ley de Protección de Datos Personales y Acción de Habeas Data.

3. El Art. N° 1 de la LPDP lo declara como un Derecho Humano, estableciendo que: "El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República".

Conforme surge del decreto reglamentario de la Ley N° 18.381[4] , decreto N° 232/2010, hay ciertos datos que en el marco de un fomento a la transparencia activa no deben ocultarse del conocimiento público, (por ejemplo los nombres de los funcionarios y sus méritos laborales o académicos) así como cualquier otro tipo de información que pudiera ser de utilidad para el conocimiento y evaluación de las funciones y políticas públicas que son responsabilidad del sujeto obligado. Pero como se ha advertido, estas disposiciones deben ser analizadas y complementadas a la luz de la normativa vigente en materia de protección de datos personales, especialmente cuando se trata de pronunciamientos de la Administración que eventualmente puedan ocasionar perjuicios de dimensiones casi inimaginables en el marco de la sociedad de la información en la que actualmente estamos insertos, especialmente en relación al denominado Derecho al Olvido, que más adelante será analizado.

IV. Sobre la comunicación, la finalidad y responsabilidad en el contenido de la información

En lo que refiere a la publicación de determinados datos personales, el art. 17 de la Ley N° 18.331 relativo a la comunicación de datos, establece que el previo consentimiento del titular no será necesario cuando así lo disponga una ley de interés general, o en los supuestos del art. 9° que ya han sido mencionados. En complemento con lo establecido y en lo relativo a la existencia de una ley de interés general, es razonable interpretar que la Ley de Acceso a la Información Pública debe ser considerada como tal a efectos de garantizar la transparencia de la administración pública. Sin perjuicio de esta referencia, como ya se ha advertido, deben mantenerse ante determinadas situaciones ciertos criterios basados en la proporcionalidad y el equilibrio, a efectos de respetar y garantizar en forma equitativa, todos los derechos e intereses en juego. Es precisamente en este sentido que la LDPD se estructura en base a determinados principios, que acompañan al principio del previo consentimiento al que ya hemos hecho referencia y que especialmente delimitan la responsabilidad de quienes poseen y/o realizan tratamiento de datos personales y cumplen la función de guiar la interpretación y resolución de todas las cuestiones que puedan suscitarse en la aplicación de las disposiciones de la norma (art. 5° in fine de la LPDP).

Entre estos principios fundamentales, se encuentran el de legalidad (art. 6) que básicamente establece que la formación de una base de datos (ya sea por parte de una persona pública como de un particular) tendrá carácter licito, cuando se encuentre debidamente inscripta ante la URCDP. Es destacable la relevancia del principio de finalidad, previsto en el art. 8 de la LPDP, establece que los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles a aquellas que motivaron su obtención, asi como que:

4. Ley N° 18.381, de 17 de octubre de 2008, regula el derecho al acceso a la información pública.

"(…) deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados (…)".

En concordancia, el art. 7° de la Ley N° 18.331 contempla la necesidad de que el tratamiento y/o comunicación de los datos sea proporcional a la finalidad que lo motiva, por ello en algunos casos la publicación de datos como el nombre, cédula de Identidad, nacionalidad, edad y dirección como hemos analizado en función a lo establecido en el art. 9 de la LPDP, no resultaría en principio, excesiva ni desproporcionada de acuerdo con las finalidades que tiene un organismo, entre ellas también la finalidad última relacionada a la necesaria transparencia que debe tener toda gestión pública. En lo que respecta a determinados datos de usuarios o actores no funcionarios de la administración pública, la URCDP se ha pronunciado en el Dictamen Nº 1/009 recaído en una Consulta relativa al Anteproyecto de Ley referido a Publicidad de Certificados que otorga el BPS[5] . En este caso, ante la posibilidad de publicar ciertos datos para brindar seguridad, se recomienda al organismo que se establezca específicamente los datos que se publicarán, que deberán ser los estrictamente necesarios para el cumplimiento de la finalidad perseguida, entendiéndose por tales RUT, razón social, habilitación o no, y vigencia. También se ha pronunciado la URCDP, respecto a que ciertos datos personales de los funcionarios pueden ser publicados, en el Dictamen N° 2/009[6] , sobre publicación en la web de otras actividades laborales declaradas por Inspectores del M.S.P, el Consejo Ejecutivo de la URCDP se expide en el sentido de publicar las demás actividades laborales de los Inspectores del M.S.P. en la medida que la mentada publicación, forma parte de las funciones propias del Organismo y la finalidad perseguida es la mayor transparencia en la gestión. En lo que respecta a los datos de los funcionarios contenidos específicamente en las resoluciones que establecen determinadas sanciones y posteriormente son publicados en el sitio web del organismo, la comunicación de dicha información puede llegar a ser excesiva con relación a la finalidad, si una vez cumplida la sanción objeto de la resolución publicada los datos del funcionario sancionado, siguen luciendo en el sitio original o aún son reconocidos por motores de búsqueda, sin un control especifico, esto sin perjuicio de las medidas de seguridad necesarias que al efecto deberían ser implementadas.

En este sentido, corresponde destacar que será el responsable del contenido (eventualmente la URSEC) quien debe decidir qué información es publicada en su sitio web, en qué forma se efectúa dicha publicación y por cuánto tiempo permanecerán esos datos disponibles en internet, así como los posibles "filtros" que dichas resoluciones puedan tener a efectos de evitar su indexación por diversos motores de búsqueda, que podrán extender en el tiempo la permanencia excesiva de una sanción caduca en el tiempo la que naturalmente pueda producir perjuicios al funcionario, titular de los datos en cuestión.

---

5. http://www.datospersonales.gub.uy/sitio/dictamenes/2009/dictamen-1-009.pdf
6. http://www.datospersonales.gub.uy/sitio/dictamenes/2009/dictamen-2-009.pdf

En consecuencia, a efectos de considerar el alcance practico de la consulta, en tanto la concordancia entre la publicación de cierta información y la finalidad por la cual la misma ha sido publicada, deberá ser analizada en cada caso por el responsable (quien toma la decisión de publicar ese contenido) adoptando al efecto medidas de seguridad necesarias para satisfacer todos los intereses en juego.

Al efecto, la información accesible sin restricciones en el sitio web de la URSEC y el tiempo que la misma se encuentre publicada, será responsabilidad de quien decide respecto del contenido de ese sitio específicamente y no necesariamente del motor de búsqueda el que precisamente buscara en forma automática la información previamente publicada.

V. Armonización entre la protección de datos personales y el deber de transparencia activa

Como se ha mencionado ut supra, es menester para el presente análisis efectuar una armonización entre los distintos derechos implicados, máxime cuando se trata de situaciones que ponen en juego una pluralidad de elementos que no necesariamente pueden ser evaluados como soluciones únicas o universales. Al efecto, deberá practicarse una ponderación de los derechos en cuestión y analizar cuál será la mejor solución para cada caso en particular, atendiendo especialmente al deber de transparencia activa que inviste a la actividad estatal moderna por un lado y a la protección de los datos personales que por otra parte el mismo Estado debe asegurar a sus habitantes. Estimo procedente citar al autor Nogueira Alcalá[7] , quien al respecto expresaba que: " (…) La correcta delimitación de los derechos y sus limitaciones externas permiten superar falsos conflictos de derechos, a su vez, cuando existe tensión entre ellos, debe asumirse que los derechos no son disyuntivos, debiendo hacerse el máximo esfuerzo por armonizarlos, debiendo ser garantizados en su contenido esencial."
Es importante señalar que en el marco de una sociedad informatizada, la publicación de datos personales en un sitio web hace que los mismos circulen alrededor del mundo, sin una delimitación cierta en el espacio y en el tiempo, dejando expuestas a las personas involucradas, que pierden el dominio de su información personal a la que otros acceden, muchas veces sin ningún tipo de restricción y con consecuencias no previsibles al momento en que dicha información es incorporada en el sitio web.

7. Nogueira, H. Teoría y Dogmática de los Derechos Fundamentales. Ed. Universidad Nacional Autónoma de México. México D.F., 2003. pp. 245 y ss. Cita realizada por Nogueira Alcalá H.en "Pautas para Superar las Tensiones entre los Derechos a la Libertad de Opinión e Información y los Derechos a la Honra y la Vida Privada". Revista de Derecho, Vol. XVII, diciembre 2004, http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S071809502004000200006&lng=en&nrm=iso Página visitada el 22 de setiembre de 2013 (22:00 horas).

Recientemente ha tomado relevancia un nuevo derecho, el que puede ser paragonado con los derechos de cancelación, oposición y supresión, denominado “Derecho al Olvido”, cuya aplicación se impone cada vez con mayor frecuencia a razón de los reclamos de las personas afectadas por la difusión de su información de carácter personal en forma indefinida en el tiempo y el espacio, situación que podría llegar a ser contemplada dentro de una resolución sancionatoria a un funcionario, que ya hubiere cumplido la sanción o que la misma hubiere sido aplicada tiempo atrás, sin perjuicio de lo cual, por el mecanismo de indexación sus datos personales lo vinculen y eventualmente lesionen en forma permanente a través de una publicación permanente en internet.

Es destacable que así como en nuestro ordenamiento jurídico las funciones del Estado no son privativas ni exclusivas de cada uno de tres clásicos poderes que integran el Estado moderno, cuando un organismo que opera en la esfera del Poder Ejecutivo como sucede en el caso en análisis con la URSEC, cumpla dentro de su ámbito de competencia con una función ciertamente jurisdiccional en su materia exclusiva, adoptando como criterio en materia de sanciones administrativas la aplicación de las Reglas de Heredia[8], adoptadas a efectos de publicaciones de información judicial en internet, efectuando para el caso en concreto un procedimiento de disociación de datos (en concordancia con lo establecido en el art. 17 D) de la Ley N° 18.331), de forma tal que la información o el asunto no pueda vincularse a persona determinada o determinable.

Cabe concluir que independientemente de la reserva que en función a las previsiones de la Ley N° 18.381 pueden realizarse respecto a las resoluciones que establezcan sanciones a los funcionarios vinculados a la URSEC, en especial consideración a la tutela de la protección de datos personales como un derecho humano fundamental especialmente previsto en la Ley N° 18.331, deberá considerarse lo ya expresado respecto a las Reglas de Heredia y la disociación de información personal contenida en dichas resoluciones, así como la adopción de las medidas de seguridad necesarias a cargo del responsable del contenido de la información y en su caso la consideración especial en la delimitación y permanencia, contemplado la finalidad de la sanción publicada, considerando especialmente que se trata de un archivo electrónico cuya permanencia indiscriminada puede ocasionar perjuicios aún más graves que la propia sanción.

8. Reglas Mínimas para la Difusión de Información Judicial en Internet, incorporados por los Poderes Judiciales de diversos países

VI. Conclusiones

1. La publicidad por parte de URSEC de las resoluciones que imponen sanciones a sus funcionarios en el marco de las obligaciones de transparencia activa, no vulnera las disposiciones de la Ley N° 18.331, en tanto se hayan considerado los principios y excepciones previstas en la norma y especialmente se haya buscado una armonización entre los derechos que se encuentran especialmente comprometidos.

2. A tales efectos, es fundamental que el tratamiento de los datos se ajuste a los principios de proporcionalidad (art. 7°) y de finalidad (art. 8°), así como a lo establecido en el art. 9° respecto al previo consentimiento informado y se adopten medidas de seguridad necesarias a los fines que motivan la consulta.

3. Es recomendable asimismo, que salvo que exista interés público en conocer la identidad de los involucrados, se aplique a las resoluciones un procedimiento de disociación de los datos, tal como se establece en el art. 17 inc. D) de la Ley N° 18.331.

4. Es necesario estar a la armonización de los derechos en cuestión en tanto la obligación de transparencia activa no impide que a través de los precitados mecanismos la URSEC como responsable de contenido, publicite en su sitio web información relativa a sanciones administrativas velando por la preservación de datos personales de sus funcionarios, quienes tendrán eventualmente derecho al olvido.

Firmado:

Dr. Federico Abbadie Gago
Derechos Ciudadanos

Informe Nº 222, de 24 de octubre de 2013.

Se informe denuncia relativa a una comunicación de datos sin consentimiento a través de la publicación en un sitio web de datos personales.

INFORME Nº		EXPEDIENTE Nº
222	2013	2013-2-10-0000337

Montevideo, 24 de octubre de 2013

I. Antecedentes

1. La Sra. AA denuncia haberse inscripto a una carrera a través del sitio web *http://www.bb.gub.uy/.* Con posterioridad, al ingresar sobre el mismo formulario con su Cédula de Identidad, se despliegan todos los datos previamente ingresados tales como teléfono celular, correo electrónico y sociedad médica. Manifiesta que realizó una prueba con la Cédula de Identidad de una amiga y sucedió lo mismo. Asimismo, explica que quiso advertir al respecto y no pudo encontrar en el sitio web ningún contacto sobre los organizadores de la carrera.

2. Conferido traslado a la Dirección Nacional de Deportes del Ministerio de Turismo y Deportes (en adelante e indistintamente DND), titular del registro del nombre de dominio, según constataciones notariales de fs. 11, solicitándole que informara si es responsable de la base de datos solicitados a los interesados y número de inscripción ante esta Unidad, así como que acreditara el cumplimiento del deber de información, el ejercicio de los derechos de acceso, rectificación, actualización, inclusión o supresión y el consentimiento expreso y escrito de los titulares para recabar sus datos de salud, de acuerdo con lo dispuesto en los artículo 13, 14, 15, y 18 de la Ley N° 18.331 de 11 de Agosto de 2008.

3. Evacuado el traslado por la Dirección Nacional de Deporte, expresó haber contratado una empresa a efectos de realizar el registro y recabar la información de los participantes. Que la información recabada debió mantenerse desde el inicio hasta la realización de la carrera, sin embargo los datos de la edición anterior se habían mantenido por más tiempo. Asimismo señaló, que luego de informados sobre el despliegue de datos en el formulario de inscripción, la aplicación fue corregida y los mismos ya no están disponibles libremente. En relación al registro de sus bases de datos, manifiesta que por ser temporales, entiende que no corresponde su inscripción y que las modificaciones de la información pueden solicitarse a través del cc@*gmail.com* que se encuentra en la sección contacto del sitio de la carrera. Agrega que no colecta datos de salud.

4. Corresponde a la Unidad Reguladora y de Control de Datos Personales (URCDP) su sustanciación, en mérito a lo dispuesto en el artículo 34 de la ante citada Ley.

II. Análisis

A. INSCRIPCIÓN WEB

La DND dispone sobre su sitio web, del servicio de inscripción en línea de la carrera “BB”. Al acceder al enlace denunciado, se visualiza un campo denominado “Inscripción”. A su ingreso, se despliega la leyenda: “Proceso de inscripción. Las interesadas en participar del evento deben ingresar en el siguiente enlace y completar los datos allí solicitados”.

El enlace *http://www.dd.com.uy* despliega finalmente el formulario de inscripción que solicita los siguientes datos: nombre, apellido, correo electrónico, cédula de identidad u otros documentos identificatorios, número de teléfono celular, fecha de nacimiento, sexo, mutualista o emergencia médica, tipo de corredor (libre, agrupado, federado).

Una vez realizado el registro, al ingresarse posteriormente un número de cédula de identidad se despliegan automáticamente el resto de los datos requeridos originalmente por el formulario.

Cabe aclarar conforme lo señala la denunciante, que cualquier persona puede acceder a la información sin necesidad de cumplir ningún requisito previo. Por lo que el proceso de registro se transforma en una consulta inversa, mediante la cual ingresando un número de cédula de identidad se obtiene la restante información mencionada, según surge de constatación notarial agregada.

Situación que fuera corregida, de acuerdo a lo manifestado por el denunciado al presentar sus descargos.

B. ADECUACIÓN A LA LEY N° 18.331

1. Comunicación de datos. - La puesta a disposición de los datos realizada por la Dirección Nacional de Deporte, denunciada y constatada en estas actuaciones, se enmarca en la definición legal de comunicación de datos personales dada por la Ley N° 18.331, desde que la consulta puede realizarla cualquier persona distinta del titular de los datos. Comunicación que deberá contar con el previo consentimiento informado de sus titulares, salvo excepciones, subsistiendo en todos los casos el requisito de cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario.

En la especie se aprecia claramente que los datos sobre número de celular, correo electrónico y sociedad médica, no pueden enmarcarse en ninguna de las excepciones previstas, así como

tampoco puede sostenerse que su comunicación responda a intereses legítimos del emisor y del destinatario, que en este último caso es cualquier persona que digite la cédula de identidad de un individuo registrado.

2. Datos sensibles. - No se comparten las manifestaciones de la DND en relación a que no recaban datos de salud de los participantes.
Al ingresar al enlace denunciado, se visualiza un campo denominado "Deslinde". A partir de su clickeo se despliega un texto titulado "Responsabilidades del Participante- Deslinde" que implica una declaración bajo juramento del participante, de no padecer afecciones físicas adquiridas o congénitas, ni lesiones que pudieran ocasionar trastornos en su salud o condiciones de vida como consecuencia de la carrera. Asimismo, declara bajo juramento haberse realizado previo a la carrera un chequeo médico y estar en óptimas condiciones físicas para participar de la misma.

Estas declaraciones constituyen, sin duda datos de salud, a la luz de las disposiciones de la LPDP y su decreto reglamentario.
Si bien dicha información no se desplegaba al ingresar la cédula de identidad, tratándose de una declaración preceptiva para participar, es pasible de asociarse a todos los participantes registrados. Relacionada la información de registro con la que surge de estas declaraciones, nos encontramos ante un colectivo identificado, segmentado por edad, sexo y domicilio, de personas que no padecen afecciones físicas adquiridas o congénitas y que se encuentran con buen estado de salud.

Lo que resulta concluyente para sostener que en este caso, claramente por descuido y desconocimiento, se recabaron y comunicaron datos sensibles sin cumplir las exigencias normativas, que disponen la necesidad del consentimiento expreso y escrito del titular para su tratamiento y el consentimiento expreso para su comunicación.

3. Principios. Finalidad. - En cuanto ideas rectoras, los principios en la materia deberán ser considerados toda vez que estemos ante tratamiento de datos personales.

Según lo dispone el inciso primero del artículo 8 de la Ley N° 18.331, los datos tratados no podrán ser utilizados para finalidades distintas o incompatibles a las que motivaron su obtención.
La finalidad que motivó la obtención de los datos objeto de esta denuncia, fue la de inscribirse a una carrera. El caso en estudio presenta por ende, una clara discrepancia entre la finalidad de registro para participar en una carrera, con la consulta de datos. Procedimientos que no son lo mismo ni pueden confundirse.
Ciertamente que no se percibe intención de la Dirección Nacional de Deporte de poner a

disposición de las personas un sistema de consulta global de sus bases de datos, sino que lo que aparentemente se buscó fue facilitar el proceso de inscripción haciendo simultáneamente un cotejo de información. Sin embargo, el resultado es el primero.

4. Derecho de Información. - Además del respeto de los principios aplicables, especial importancia reviste el cumplimiento de las disposiciones del artículo 13 de la LPDP que regula el derecho de información frente a la recolección de datos. Extremo que notamos falta en este proceso, el que debería contener la siguiente información enunciada en forma expresa, precisa e inequívoca:

- finalidad para la que serán tratados los datos y quiénes pueden ser sus destinatarios o clase de destinatarios;
- existencia de la base de datos de que se trate y la identidad y domicilio del responsable;
- carácter facultativo u obligatorio de los campos del formulario propuesto;
- consecuencias de proporcionar o no los datos o de su inexactitud (por ejemplo, la imposibilidad de participar de la carrera);
- posibilidad y forma del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

5. Inscripción de base de datos. - El hecho que una base de datos se mantenga por un lapso corto de tiempo no exime a su responsable de la obligación de registro ante esta Unidad, conforme los artículos 24 de la LPDP y 15 y siguientes del decreto N° 414/009.

III. Conclusiones

1. El sistema de registro en estudio no se ajusta a las disposiciones de la Ley N° 18.331, en virtud de no cumplir los extremos requeridos por los artículos 9, 13, 18 y 24 de la norma y por desvirtuar la finalidad de registro en consulta.
2. Se aconseja exhortar a la Dirección Nacional de Deporte la inmediata adecuación de sus procesos de inscripción en línea a las disposiciones de la LPDP, poniendo especial atención al tratamiento de la información de carácter sensible. A tales efectos deberá:
   - incluir un instructivo de registro o documento análogo con la información enunciada en el artículo 13 de la Ley N° 18.331, en cuanto corresponda,
   - evitar el despliegue automático de información a partir del ingreso de un dato.
3. Asimismo, se recomienda intimar el registro de sus bases de datos en el plazo de 30 días corridos, bajo apercibimiento de ser sancionada.

Es todo cuanto tengo que informar.

Firmado:
Dra. Bárbara Muracciole
Derechos Ciudadanos

Informe Nº 245, de 19 de noviembre de 2013.

Se informa denuncia relativa a acciones publicitarias con bases de datos ilícitas.

INFORME Nº		EXPEDIENTE Nº
245	2013	2013-2-10-0000132

Montevideo, 19 de Noviembre de 2013

I. Antecedentes

1. AA presenta denuncia contra la empresa de telefonía BB, en virtud "que realiza acciones publicitarias telefónicas con bases de datos obtenidos de manera ilegal".

2. Al evacuar el traslado, BB S.A. informa que "la línea telefónica número 96128533 se encuentra asociada a la cuenta número 2…, bajo la titularidad de la empresa CC", a la cual solicita se le confiera vista.

De acuerdo a lo peticionado, se confiere vista en dos oportunidades, quedando en ambos casos truncada la notificación, en función de resultar incorrectos los domicilios aportados por BB.

3. Siendo que la denuncia fuera presentada contra BB y no contra la empresa CC, y en virtud que las llamadas con fines publicitarios se realizaron en nombre de la denunciada, extremo que no fuera negado ni controvertido en oportunidad de presentar sus descargos, previa prosecución de estas actuaciones y conforme lo preceptuado en el artículo 34 de la Ley N° 18.331, se solicitó a BB que:

- agregara la grabación de la llamadas recibidas el día 5 de Abril de 2013 entre las 14:00 y las 15:00 horas por el Call Center del cual el Sr. DD es supervisor. Particularmente, la llamada recibida de AA y atendida por el Sr. DD;
- especificara el vínculo entre BBy el Call Center aludido, así como con el Sr. DD; acompañando la documentación acreditante (exhibiendo original o testimonio notarial);
- explicara el vínculo contractual que mantenía con la persona física o jurídica titular del número 09…, agregando la documentación acreditante (exhibiendo original o testimonio notarial);
- justificara la utilización del número de teléfono celular del denunciante para su tratamiento con fines publicitarios, probando el consentimiento u origen de fuente pública en su caso, en el entendido que no se trataba de un cliente de la empresa denunciada ya que su número correspondía a otro operador de telefonía celular.

4. De la información y documentación solicitada, la denunciada exhibió un Contrato de Agencia con EE, Sociedad de Hecho (sin sus Anexos) y presentó copias de los telegramas colacionados que comunicaban la rescisión de dicho Contrato. Respecto del resto, expresó que

“no mantuvo vínculo alguno con un Call Center y tampoco con una persona que el denunciante dice que se llama Rafael Castro. Por tanto no existe documentación a aportar, siendo su único vínculo el de agencia mencionado” y solicitó por tercera vez que se confiriera vista a Facubon en una nueva dirección postal, en la que tampoco fue posible realizar la notificación.

5. Corresponde a la Unidad Reguladora y de Control de Datos Personales sustanciar la presente denuncia, en mérito a los cometidos que le fueran atribuidos en la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de Agosto de 2008.

II. Análisis

1. Tratamiento. Responsabilidad.- BB deslinda toda posible responsabilidad sobre los hechos denunciados en EE, Sociedad de Hecho (CC), en virtud del contrato de agencia que los unía, manifestando que se trata de empresas independientes y por ello no le era posible conocer los aspectos relacionados con la recolección, obtención y tratamiento de datos personales que realizaba. No obstante, la llamada objeto de estas actuaciones se realizó en nombre de BB, extremo que -reitero- no fuera negado ni controvertido por ésta.

Asimismo, del objeto del Contrato agregado, surge que el Agente realizaba promociones, gestiones y obtenciones de pedidos por cuenta y orden de BB (cláusula 2.1) y que debía elaborar y mantener un registro de clientes potenciales con el nombre, documento de identidad, dirección, teléfono y “cualquier otra información que señale BB” y entregar en las instalaciones de esta última, luego de la firma de la solicitud de servicio “la totalidad de los documentos originales diligenciados junto con fotocopias de los documentos de identidad y aquellos que acrediten la representación legal en caso de tratarse de personas morales” (cláusula 6.5).

Por otra parte, BB exigía al Agente registrar sus actividades (registros de clientes, solicitudes de servicio, modificaciones) mediante pautas específicas, dejando expresa constancia en el Contrato, que dichos registros serán propiedad de AMWU y deberán estar a su disposición hasta tres años después de la terminación del Contrato de Agencia (cláusula 6.9).

De las disposiciones transcriptas y de una lectura integral del Contrato, se desprende que la información personal utilizada por el Agente para su actividad es propiedad de la denunciada y su tratamiento se realizaba por cuenta y orden de la denunciada. Por lo que BB es responsable en sede de protección de datos conforme lo dispuesto en los artículos 4 literales H) y K) y 12 de la LPDP), siendo el Agente encargado de tratamiento.

2. Consentimiento. Falta.- Se advierte que BB no probó contar con el consentimiento del denunciante para utilizar su número de teléfono celular, o su origen de fuente pública, de

acuerdo con lo dispuesto en los artículos 9 y 21 de la Ley N° 18.331, lo que además de ser su obligación[9] , le fuera expresamente solicitado a fs. 52 de los presentes. Por lo que nos encontramos ante una situación de utilización de datos personales sin consentimiento de su titular.

3. Deber de informar. Incumplimiento.- De las manifestaciones del denunciante respecto a que "El supervisor también rehusó darme el nombre de la empresa que realizaba este servicio y me cortó el teléfono ante la pregunta", que tampoco fueran objeto de controversia o prueba en contrario por la denunciada, se aprecia el incumplimiento del deber de informar dispuesto en el artículo 13 de la Ley N° 18.331.

4. Inscripción de Base de Datos.- Estas actuaciones, además, arrojaron irregularidades en los registros de bases de datos de AMWU ante la URCDP. Según constataciones internas, la referida empresa posee inscriptas las siguientes bases de datos:

4.1 **"Proveedores" N° B 6977.-** Tramitada en Expediente N° 2012-2-10-…, continente de datos sobre sus proveedores.

4.2 **"Videovigilancia" N° 6978.-** Tramitada en Expediente N° 2012-2-10-…, continente de datos de imagen/voz obtenidos por videovigilancia.

4.3 **"Empleados" N° B 6979.-** Tramitada en Expediente N° 2012-2-10-…, continente de datos de los empleados de la empresa.

4.4 **"Clientes" N° 6980.-** Tramitada en Expediente N° 2012-2-10-…, continente de datos de sus clientes.

De los nombres asignados y descripciones presentadas, se desprende que ninguna contempla ni puede considerarse abarcativa de los contratos de agencia o información derivada, por lo que se advierte el tratamiento de información personal no declarada ante esta Unidad, que se suma a la omisión de declarar al Agente como encargado de tratamiento.

5. Debido proceso. Derecho de defensa.- El denunciado evoca reiteradamente caros preceptos del Derecho como son el debido proceso y el derecho de defensa, deslisando consideraciones equivocadas y desafortunadas a juicio de esta informante, por cuanto sugieren que en estos obrados la Administración se ha apartado del debido proceso.

Así, por ejemplo, expresa: "ya que no estamos en sede judicial, por tanto mi mandante no tiene la carga de contradecir o controvertir hechos"; "es a la Administración a la que le compete

9. "Corresponderá al responsable de la base de datos o el tratamiento recabar y guardar la prueba de la existencia del consentimiento o de la negativa a darlo, por parte del titular, a través de cualquier medio conforme a derecho." Inciso 3 del artículo 6 del Decreto N° 414/2009.

sustanciar el procedimiento administrativo correspondiente que le permita determinar la verdad material de los hechos, no pudiéndose respaldar únicamente en una simple denuncia por un particular, so pena de vulnerarse el derecho de debido proceso y de defensa"; "el criterio esbozado en el informe jurídico señalado -que refiere a la no contradicción de los hechos denunciados por parte de BB en su primera comparecencia- sólo sería procedente en caso de la resolución sancionatoria firme".

Sostener que al denunciado en via administrativa no le corresponde controvertir los hechos implica, lisa y llanamente, desconocer principios generales del Derecho aplicables al procedimiento administrativo y expresamente recogido en el Decreto N° 500/991, de 27 de setiembre de 1991.

En palabras del Profesor Juan P. Cajarville Peluffo, el principio del debido procedimiento o derecho a defenderse recogido en el artículo 2 *"se explicita en el artículo 5 que dispone que los interesados gozarán de todos los derechos y garantías inherentes al debido proceso, de conformidad con lo establecido por la Constitución de la República, las leyes y las normas de Derecho Internacional aprobadas por la República, lo cual implica un procedimiento de duración razonable que resuelva sus pretensiones."*[10]

"El derecho a defenderse no se limita a la posibilidad de ser oído antes de dictarse resolución; comprende también el derecho a ser notificado de la existencia del procedimiento, a conocer el contenido de las actuaciones, a comparecer reclamando lo que se entienda corresponder con el patrocinio letrado que se juzgue conveniente, a que se diligencie la prueba admisible, pertinente y conducente que se ofreciera, a que se resuelvan las pretensiones en un procedimiento de duración razonable y a que se dé conocimiento de los motivos de la decisión de la administración (ver, sobre todo, Cap. Sexto, 1, 5; IV, 1; V y VII). Por todo ello, el art. 171 no debe interpretarse como una norma excepcional aplicable sólo a los funcionarios públicos y suceptible de interpretación a contrario en los demás casos, sino como la enunciación en el caso de un principio general que rige para toda persona imputada de una ilegitimidad". [11]

"El principio de contradicción (art. 2 ap. j) también es expresión de este derecho fundamental cuando existe en un procedimiento más de un interesado con intereses encontrados (arts. 17 y 153) (véase Cap. Tercero, II, A; y Cap. Sexto, IV, 1)." [12]

---

10. Juan P. Cajarville Peluffo. Procedimiento Administrativo en el Decreto 500/991, Montevideo, Ediciones Idea, 1992, págs. 20 y 21.
11. Op. cit., pág. 21.
12. Op. cit., pág. 21.

Vemos entonces, que el principio de contradicción surge del debido proceso y derecho de defensa e informa todo el procedimiento administrativo y no solo la etapa recursiva, como equivocadamente señala la denunciada. Por lo que la solicitud de información y documentación, así como las vistas conferidas por la Administración en estas actuaciones, no hacen otra cosa que brindar a los interesados la oportunidad de realizar sus descargos, a fin de reunir los elementos necesarios para alcanzar la verdad material mediante la sustanciación de la denuncia, en apego absoluto a los principios y derechos referidos.

6. En definitiva, se constata que el denunciado vulneró la normativa de protección de datos, particularmente los artículos 9, 13, 21 y 29 de la Ley N° 18.331.

7. El denunciado ha sido apercibido por esta Unidad mediante Resolución N° 18 de 17 de Junio de 2009, recaída en Expediente N° 007/2009.

III. Conclusiones

1. Se sugiere sancionar a BB S.A. con pena de multa, por vulnerar lo dispuesto en los artículos 9, 13, 21 y 29 de la Ley N° 18.331.
2. Téngase presente el cabal cumplimiento del debido proceso en estas actuaciones, desaprobándose las expresiones de BB en sentido contrario.

Es todo cuanto tengo que informar.

Firmado:
Dra. Bárbara Muracciole
Derechos Ciudadanos

Informe Nº 277, de 30 de diciembre de 2013.

Se informa consulta de la Intendencia de Florida sobre comunicación de datos personales solicitados por edil departamental.

INFORME Nº		EXPEDIENTE Nº
277	2013	2013-2-10-0000562

Montevideo, 30 de diciembre de 2013

I. Antecedentes

La consulta ha sido realizada por la Intendencia Departamental de Florida y refiere a la entrega de copia de la documentación entregada por parte de determinado contribuyente, con el fin de realizar el trámite de empadronamiento de un vehículo.

En la sección Trámites en el sitio de la Intendencia de Florida *(http://www.imf.gub.uy/wps/wcm/connect/imf/imf/servicios_al_ciudadano/informacion/tr_aacute_mites+frecuentes/empadronamientos* Página visitada el 30/12/13), se indica que para el empadronamiento de ciertos vehículos como Motos, Autos, Camiones, Acoplados, Trailers, Ómnibus, la documentación que se requiere es la siguiente:

"- Carta de la casa vendedora (certificada)
- Certificado de Importación (cert. Industria)
- Inspección Técnica
- Cédula de Identidad
-Certificado de Residencia
- Si no es el propietario Carta Poder certificada".

En definitiva, la Edil está solicitando tener acceso a toda la documentación antes descripta, relacionada al nombre y demás datos personales de determinado contribuyente, interesado en realizar dicho trámite ante la comuna.

II. Análisis y marco jurídico de aplicación

a. Derechos a considerar

Las intendencias son sujetos obligados en el marco de lo previsto por la Ley N° 18.381, que si bien establece la obligación de brindar acceso a la información que les es solicitada dentro del plazo estipulado, también obliga a analizar y clasificar la información que se encuentra amparada por alguna de las excepciones.

En la petición analizada, hay datos que deben ser considerados información confidencial, pues se trata de datos personales que requieren previo consentimiento informado según se establece en el art. 10 Num. II de la Ley N° 18.381.

Por otra parte, el art. 1° de la Ley N° 18.331 (LPDP), reconoce que el derecho a la protección de datos personales es inherente a la personalidad humana, por lo que está comprendido en el art. 72 de la Constitución Nacional.

Nuestra Constitución a su vez, también contiene otras normas que garantizan otros derechos relacionados, como el derecho a la libertad[13] y a la privacidad[14] ., por ello, si bien es cierto que el pedido de informes realizado por un Edil Departamental se enmarca en lo establecido en el art. 284 de la Constitución, corresponde tener presente, que la LPDP consagra un derecho humano y un sistema de protección especial que se sustenta en la propia Carta Magna.

En definitiva, es necesario equilibrar los derechos e intereses en juego, a la luz de los principios que estructuran la protección de datos personales, pero muy especialmente tener en cuenta los principios de finalidad y de proporcionalidad.

b. Principio de finalidad y juicio de proporcionalidad

A la hora de brindar acceso a información personal que por definición pertenece a los particulares, -pero que por determinado motivo se encuentra en poder de un organismo público (en este caso la Intendencia de Florida)-; indefectiblemente debe realizarse un juicio de proporcionalidad, basado en la idoneidad, la necesidad y el equilibrio de derechos.

Esto significa que debe existir una justificación que resista ese juicio y muestre como imprescindible la utilización de esa información, por ejemplo para investigar un delito, evitar un peligro inminente o contribuir a determinada investigación judicial. Si este fuera el caso, la información debería ser solicitada a través de la justicia.

Por otra parte, la Intendencia recoge esa información para brindar un servicio específico, o sea para determinada finalidad que debe ser respetada (art. 8°).

Además, la LPDP en su artículo 9° c) enumera una serie de datos personales que no requieren el previo consentimiento informado para su comunicación (nombre y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento), pero como vemos, en el caso la información solicitada excede este listado e incluye otros datos o información que sí lo requiere.

Por otra parte en el art. 17, respecto a la comunicación de datos personales, se exige para su legitimidad, la conjunción simultánea del 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. En el caso, se presume, dado el tenor de la consulta, que no existe interés en el titular de los datos así como tampoco su consentimiento.

---

13. Artículo 7º. Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad. Nadie puede ser privado de estos derechos sino conforme a las leyes que se establecen por razones de interés general.

14. Artículo 10. Las acciones privadas de las personas que de ningún modo atacan el orden público ni perjudican a un tercero, están exentas de la autoridad de los magistrados. Artículo 28. Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general.

Por otra parte, hay que considerar que en el mismo artículo se enumeran una serie de excepciones que prima facie no aplicarían al caso: existencia de una ley de interés general, presupuestos del art. 9°, datos de salud para prevenir emergencias, aplicación de procedimiento de disociación de la información.

c. La URCDP ya se ha pronunciado sobre este tema

Cabe recordar por otra parte, que el Consejo Ejecutivo de la URCDP ya se ha expresado en forma negativa en cuanto a brindar la información personal de determinados beneficiarios de servicios del Estado.

En tal sentido en el Dictamen N° 15 del 15 de setiembre de 2011, ante la consulta presentada por el Fondo de Solidaridad, acerca de si debía o no informar la identidad de los beneficiarios de las becas que otorga la Institución, el Consejo dictaminó que "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".

Mediante el Dictamen N° 10 de 2012, ante consulta formulada por la Intendencia de Rocha respecto a la solicitud de acceso a información personal planteada por un Edil Departamental, la URCDP indica que "sólo procede la divulgación de información disociada de los titulares al amparo de lo previsto por el Literal D del artículo 17 de la LPDP", salvaguardando la identidad de los beneficiarios del servicio de refugio que brinda esa comuna.

Por su parte, en consulta similar a la ya analizada, formulada por la Unidad de Acceso a la Información Pública, en razón de la solicitud de acceso planteada ante la Intendencia de Montevideo; en el Dictamen N° 12 de 7 de junio de 2012 indica que "en cuanto a la posibilidad de informar la identidad de los propietarios de los vehículos, procede la divulgación de información disociada de los titulares, al amparo de lo previsto por el literal D del artículo 17 de la LPDP".

III. Conclusiones

Cabe concluir entonces que, desde el punto de vista de la protección de datos personales, la Intendencia de Florida sólo estaría legitimada a entregar al solicitante, información relacionada con el empadronamiento de vehículos en forma general y disociada de los titulares del trámite.

Respecto a la posibilidad de entregar copia de toda la información de un contribuyente en particular, debe considerarse que no corresponde legalmente ya que vulnera el derecho a la protección de datos, y no se ajusta a los principios de proporcionalidad y de finalidad previstos en la Ley N° 18.331.

Firmado:

Dra. Graciela Romero
Derechos Ciudadanos

Informe Nº 4, de 20 de enero de 2014.

Se informa denuncia sobre instalación de cámaras para video vigilar a los trabajadores.

INFORME Nº		EXPEDIENTE Nº
4	2014	2013-2-10-0000570

Montevideo, 20 de enero de 2014

I. Antecedentes

El 20 de diciembre de 2013, AA y BB, denuncian a CC S.R.L. (en adelante la empresa), alegando que se vulneran sus derechos al ser video vigilados en el lugar de trabajo, a partir de que ambos se han afiliado al sindicato de Artes Gráficas.

Alegan que a partir de esta decisión de afiliarse al sindicato, (aclaran que son los primeros en hacerlo en la historia de la empresa), comienza una represión sindical, siendo una de las modalidades de ésta, el seguimiento y el control de todos sus movimientos y de sus diálogos, a través de la instalación de un sistema de video vigilancia.

Afirman que los encargados de la empresa, hacen referencia en forma permanente a la información que obtienen de las conversaciones mantenidas por ellos dentro de la sección de trabajo (porque las escuchan a través del sistema), e incluso fue despedido un trabajador que fue filmado manteniendo una conversación con dirigentes del sindicato.

Indican también, que la base de video vigilancia no está registrada ante la URCDP y no cuentan con carteles de advertencia a la vista, así como nunca se les informó sobre su puesta en funcionamiento.

Por su parte, con fecha 27 de diciembre de 2013, la denunciante AA, agrega documentación que prueba que ha ejercido el derecho de acceso ante la empresa, solicitando copia de todos sus datos personales y especialmente de los registros de una de las cámaras que apunta hacia la reja de acceso. Indica que pasado el plazo de 5 días hábiles previstos en la Ley, no recibe la totalidad de la información solicitada.

A folio N° 29 se adjunta documento donde consta que se entregó a la denunciante parte de la información solicitada, pero hay una nota al pie donde ésta, al firmar deja constancia de que falta parte de la misma (se trata de un documento agregado por la defensa de la empresa).

Es pertinente indicar a su vez que, a folio electrónico 43 y siguientes del expediente, surge agregado CD -ROOM por parte de los denunciantes. Del contenido del mismo se procede a de realizar la comprobación notarial de las imágenes y sonidos.

Del acta de constatación surge que se filma con imagen y sonido diferentes situaciones del lugar de trabajo, aunque se advierte que algunos tramos cuentan dicho sonido y otros no. Esto indica que en definitiva, se selecciona el alcance que le puede dar a dicha filmación, y si desea o no brindar acceso al sonido y a la voz de los involucrados.

A folio N° 30 se presenta la empresa negando la persecución sindical e indicando la falsedad de las denuncias, puesto que la finalidad de las cámaras es el control de la actividad productiva y la seguridad de las instalaciones.

Agregan que el tiempo de conservación de las imágenes y micrófonos es de 24 horas, pero que también se realiza un respaldo en CD únicamente de *"eventos puntuales y relevantes para ser utilizados como medios de prueba" y que estos datos "están a disposición de los titulares".*

Afirman que el consentimiento previo ha sido obtenido a través de la colocación de los adhesivos de la URCDP en lugares visibles del establecimiento, tanto para trabajadores como clientes y proveedores, así como la empresa ha cumplido con el derecho de acceso de ambos denunciantes. Se adjunta como prueba copia del recibo de entrega de CD con datos personales, pero no se adjunta ningún tipo de prueba (fotos, documentación) que indique la ubicación de las cámaras ni de los adhesivos.

II. Análisis de los principales aspectos de la denuncia

A) Sobre la ponderación de derechos

La URCDP debe realizar un balance entre el derecho que tiene la empresa a proteger sus bienes e instalaciones y garantizar la seguridad, y el derecho a la intimidad y a la protección de datos personales de los trabajadores, a la luz de los principios que inspiran la Ley N° 18.331, sobre todo los de consentimiento, finalidad y proporcionalidad (art. 5° parte final)..

Tal como se expresa en el Dictamen N° 10/010 de 16 de abril de 2010, la video vigilancia puede tener *"como principales finalidades la protección de las personas físicas, del derecho de propiedad, la tutela del orden público, la detección y prevención de delitos, así como otros intereses legítimos".* No obstante ello, es claro que el sistema no puede ser utilizado para vulnerar el derecho a la vida privada y a la protección de datos personales de los trabajadores.

Para determinar este punto, la utilización del sistema debe ser analizado en el marco del principio de proporcionalidad a efectos de descartar, por ejemplo, ciertos lugares que no pueden ser video vigilados como son los vestuarios, comedores, cocinas y baños de los trabajadores.

Tampoco podrían ser utilizados los registros que se obtengan de la vía pública, concretamente de la zona que coincide con el ingreso a la empresa (todavía no se estaría dentro de la misma),

pues ello sería ilegal y desproporcionado. Esta observación es pertinente dado que una de las denunciantes, solicita acceder a los registros de una de las cámaras que filma hacia la reja de ingreso a la empresa.

Por otra parte, la empresa indica en los descargos que el consentimiento previo ha sido obtenido a través de la colocación de los adhesivos de la URCDP en lugares visibles del establecimiento, tanto para trabajadores como clientes y proveedores, pero este punto no es acreditado por parte de la empresa con agregado de fotos de los logos o copia del aviso dónde se cumple con informar a los trabajadores. Tampoco se indica a partir de cuándo se informa.

Todas estas apreciaciones acerca de los límites de la videovigilacia en el ámbito laboral se extraen, tanto de la Ley N° 18.331 y su decreto reglamentario, explicitadas en el Dictamen N° 10 de la URCDP ya citado, así como de otros documentos relativos al tema y reseñados en este informe.

Concretamente en el Dictamen de la URCDP N° 10/010 se considera que la video vigilancia es *"toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo".*

Se agrega que "esta captación o grabación de imágenes constituye información personal, por lo que resulta de aplicación la normativa vigente sobre protección de datos personales, a cuyos efectos corresponde tener en cuenta los diversos aspectos comprendidos, a lo que puede ser video vigilado, de qué forma, qué principios son aplicables y si se deben registrar los resultados de la videogilancia, entre otros".

Este Dictamen establece también que debe observarse que las mismas *"no tengan finalidades violatorias de derechos humanos o contravengan la moral pública"*, por ello de acuerdo con el principio de finalidad, los sistemas de video vigilancia deben tener consignado por escrito u otro medio análogo las finalidades para las que se utilizan, y este uso debe quedar estrictamente limitado a las finalidades expresamente consignadas. Agrega a su vez que, de acuerdo con el principio de veracidad (artículo 7° de la LPDP), estos sistemas deben ser subsidiarios y sólo pueden ser utilizados cuando no exista otro medio menos lesivo de la intimidad de las personas.

Estas apreciaciones son coincidentes con las realizadas por la Organización Internacional del Trabajo (OIT), en el Documento "Repertorio de recomendaciones prácticas de la OIT", adoptado en la reunión de expertos en Ginebra en 1996, sobre la protección de la vida privada de los trabajadores, donde se señala que el tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita y limitarse exclusivamente a

asuntos directamente pertinentes para la relación de empleo del trabajador.[15]

También hay que considerar que en nuestro país los tribunales han entendido que hay cierto margen de control al que tienen derecho los empleadores, pero sin extralimitarse. Por ejemplo en la Sentencia del Juzgado Letrado de Trabajo de 1º Turno Nº 4 de 7 de marzo de 2006[16] , se expresa que *"la propia naturaleza de la relación subordinada da lugar a que la eficacia de estos derechos pueda verse limitada. Así se ha sostenido, que el poder de vigilancia, y contralor de los trabajadores por parte del empresario vulnera el derecho a la intimidad cuando se extralimita, cuando los medios electrónicos controlan al trabajador y no a la actividad que este realiza. Los tribunales españoles aplican, a la hora de admitir o no el uso de estos medios para el control de los trabajadores, un juicio de proporcionalidad (idoneidad, necesidad y equilibrio). En este sentido, debe existir una justificación para la utilización de esos medios de control (...)"* .

Incluso en aquellos casos donde la empresa pretende controlar el funcionamiento así como detectar conductas inapropiadas de los trabajadores, como se indica en los descargos para justificar que se realiza un respaldo en CD únicamente de "eventos puntuales y relevantes para ser utilizados como medios de prueba", corresponde que se considere el principio de proporcionalidad.

Ilustra esta necesidad lo expresado por parte de la Sr. Juez Dr. Néstor Valetti, titular del Juzgado Letrado de Primera Instancia en lo Penal Especializado en Crimen Organizado de 1er. Turno, en la Sentencia dictada en autos IUE: …, respecto a que la vigilancia electrónica permanente, como escuchas telefónicas por ejemplo, "no es admisible (que) para pequeños delitos se constituya en la reina de las pruebas, porque de lo contrario estamos sometidos a un estado de vigilancia, donde por un precio módico obtenemos la prueba: es la investigación policial la que dará lugar a la escucha y no la escucha la que dará lugar a la investigación".

Esto quiere decir que en definitiva, siempre hay límites legales a considerar, los hay aun en medio de circunstancias tan claras de lucha contra ciertos tipos de delitos, que hacen a una investigación judicial como la que trata la sentencia de referencia, con más razón aún en un ámbito laboral.

---

15. Repertorio de recomendaciones prácticas de la OIT adoptado en Ginebra del 1º al 7 octubre 1996, en una reunión de 24 expertos sobre la protección de la vida privada de los trabajadores, en cumplimiento de una decisión tomada por el Consejo de Administración en su 264ª sesión en noviembre de 1995. http://www.avpd.euskadi.net/s045249/es/contenidos/informacion/documentos_otros/es_docum/adjuntos/OIT_recomendaciones.pdf.

16. Sentencia del Juzgado Letrado de Trabajo de 1º Turno Nº 4 de 7 de marzo de 2006.- Se resuelve el tema del mail en el trabajo y la protección de datos personales en relación a archivos con fotografías del actor. http://www.jurisprudenciainformatica.gub.uy/jurisprudencia/ficha.jsp?id=96

Por tanto, en principio, siempre que los trabajadores sean informados debidamente, es legítimo instalar cámaras para controlar la actividad e instalaciones dentro de la empresa, pero hay que tener en cuenta la proporcionalidad entre la finalidad y el tratamiento tal como se ha señalado antes, sobre todo respecto a la ubicación de las mismas, el alcance de los datos que se recopilan, para qué son utilizados y la forma en que se avisa a los trabajadores (arts. 6°, 7°, 8°, 9°, 12 y 13 de la LPDP.)

B) Sobre las obligaciones de los responsables

Según el Dictamen de la URCDP N° 10/010 ya mencionado, los responsables de las BD de video vigilancia son responsables por el cumplimiento de la normativa que los regula, sobre todo en lo referido a la protección de los datos.

Para ello deberán actuar con la debida reserva o sea adoptar medidas de seguridad para garantizar que solamente las personas autorizadas accedan a ellos., mantener la información en forma confidencial, por la cual el responsable debe ser el custodio de las imágenes, así como garantizar que el titular de los datos pueda ejercer su derecho de acceso, e informar a las personas que sus imágenes están siendo captadas.

C) Sobre el tratamiento de datos de afiliación sindical

El art. 4° E) de la Ley indica que los datos sensibles son aquellos que revelen el origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

Como se observa los datos relativos a la afiliación sindical de los trabajadores son considerados por la Ley datos sensibles y por eso tienen una regulación especial (art. 18), teniendo presente que es información que eventualmente puede ser utilizada para discriminar a las personas.

En este sentido, la Ley advierte que salvo las excepciones previstas, queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles.

D) Sobre el deber de inscripción

La empresa afirma que el tiempo de conservación de las imágenes y micrófonos es de 24 horas, pero que también se realiza un respaldo en CD únicamente de “eventos puntuales y relevantes para ser utilizados como medios de prueba” y que estos datos “están a disposición de los titulares”.

Esto sin dudas refiere a la existencia de una base de datos que contiene imágenes y audios, por ende deben ser inscripta en el registro de la URCDP. La Ley es clara al respecto, una base

de datos se considera ilegal sino se encuentra debidamente registrada (arts. 6°, 28 y 29 de la ley, arts. 15 a 20 del decreto N° 414/009).

En este sentido, con fecha 21 de enero se ha presentado ante ésta unidad un formulario de registro de base de datos a nombre de la empresa CC S.R.L, el que ha sido identificado con el número de expediente: …, y se le ha observado que contiene "DATOS DE CLIENTES DATOS PERSONALES DE LOS EMPLEADOS DE LA EMPRESA y FILMACIONES DE SEGURIDAD" y de acuerdo con el principio de finalidad consagrado en el artículo 8 de la Ley se estaría ante la presencia de tres bases de datos ("clientes", "empleados" y "videovigilancia"). Por consiguiente, se deberá presentar un formulario por cada una de ellas.

III. A modo de conclusión

En definitiva, la imagen, la voz y el sonido asociados a ella, son datos personales y su tratamiento debe estar sujeto a la normativa de protección de datos personales.

En cuanto al consentimiento, en el caso que se analiza no sería necesario obtener el consentimiento de los trabajadores afectados por el sistema de video vigilancia pues el art. 9 de la Ley que establece una serie de excepciones, entre ellas, en el Numeral D), establece que si esos datos derivan de una relación contractual por ejemplo, y son necesarios para su desarrollo o cumplimiento no se exige recabar el mismo en forma expresa. Esta excepción sería aplicable al caso.

Sin perjuicio de lo anterior, la instalación de cámaras y videocámaras, tendrá que respetar los demás requisitos exigidos por la legislación vigente en la materia, y para ello la empresa deberá:

a) Informar expresamente a los trabajadores, pues de esta forma la video vigilancia pasa a formar parte de la propia relación laboral y el tratamiento de los datos pasa a ser necesario para su adecuado desenvolvimiento de la misma (art. 13 de la Ley N° 18.331).

b) Informar en forma expresa, precisa e inequívoca acerca del mecanismo que se utilizará, la finalidad que tiene y el lugar que será video vigilado (art. 13 de la Ley N° 18.331).

c) Utilizar los datos sólo para la finalidad para la cual son recabados, esto quiere decir que no podrán ser utilizados para fines distintos (art. 8 de la Ley N° 18.331) y deben eliminarse una vez cumplida la finalidad para la cual se han obtenido, salvo que se justifique su conservación, por ejemplo en caso de constatarse un delito. En este sentido, debe observarse que las bases de datos "no tengan finalidades violatorias de derechos humanos", o que no se limiten en forma única y exclusiva, al almacenamiento de datos que revelen directa o indirectamente datos

sensibles (en el caso por ejemplo datos referidos a la afiliación sindical de los trabajadores).

d) Respetar los espacios privados como baños, cocinas o vestuarios, pues la video vigilancia en estos casos afecta la intimidad y privacidad y no se ajusta al principio de proporcionalidad (adecuación del medio utilizado al fin que se persigue), que debe contemplarse para que la misma sea legítima (art. 1° y 6° num. 2 de la Ley N° 18.331).

d) Garantizar la seguridad y confidencialidad de las imágenes que se obtienen (art. 11 de la Ley N° 18.331). Para ello debería limitarse el acceso a un número lo más limitado posible de personas.

e) Inscripción de las bases en el registro que a tales efectos lleva la URCDP (arts. 6°, 28 y 29 de la ley, arts. 15 a 20 del decreto N° 414/009).

En este sentido, además de asesorar a la empresa acerca de todas las obligaciones que emergen de la normativa vigente, se recomienda al Consejo aplicar la sanción que estime conveniente a CC por infracción a los arts. 6°, 13 y 14 de la LPDP y art. 17 del Decreto N° 414/009, esto es por no haber inscripto sus bases datos en tiempo y forma ante la URCDP, no informar en los términos y alcances establecidos en la art. 13 de la Ley a los trabajadores, y no garantizar en forma completa el derecho de acceso de la denunciante, según los elementos que se han agregado al expediente por parte de ambas partes.

Atendiendo a la posibilidad de que recaiga una resolución no favorable a los intereses de la denunciada, se solicita darle vista previa en los términos del art. 75 del Decreto Nº 500/991 de 27 de setiembre de 1991.

Firmado:
Dra. Graciela Romero
Derechos Ciudadanos

Informe Nº 36, de 14 de marzo de 2014.

Se informe denuncia sobre ejercicio del derecho de acceso.

INFORME Nº		EXPEDIENTE Nº
36	2014	2013-2-10-0000923

Montevideo, 14 de marzo de 2014

I.- Antecedentes

El Sr. AA, se presenta ante ASSE el 31 de julio de 2012 (según lo explica en el formulario de denuncia de la URCDP), a efectos de solicitar acceso a "toda documentación en poder del Departamento de Certificaciones Médicas relativas a su persona" (listados de certificaciones, historia clínica y demás vinculadas y en poder del mismo). Funda su derecho en el art. 14 de la Ley N° 18.331.

Denuncia que en varias oportunidades concurrió a ese lugar con el fin de acceder a sus datos, y se le informó que quien debía autorizar la entrega era el Dr. CC. Al día de la presentación de su denuncia ante la URCP, o sea al 26 de diciembre de 2012, esa información no le había sido proporcionada bajo diversas excusas, y recién se le brindó acceso a la misma el 5 de setiembre de 2013 (folio N° 41).

A folios electrónicos N° 30 y N° 66 del expediente se presenta ASSE, alegando que el Sr. AA siempre ha tenido la posibilidad de acceder a la documentación y dictámenes médicos expedidos en los expedientes que refieren a su persona, a efectos de cumplir con el debido proceso.

Agrega que dicho funcionario ya ha realizado múltiples peticiones ante ASSE, y que siempre se han formado expedientes con el fin de analizarlas y obtener el pronunciamiento de la administración, al amparo de lo dispuesto en el Decreto 500/91.

Observan que ya hay pronunciamiento de la URCDP y de la UAIP acerca de una denuncia presentada por el Sr. AA: Resolución N° 93/2013 (exp. 2012-2-10-…) y N° 33/2013 (Exp. 2013-2-10-…), respectivamente.

En definitiva, ASSE considera que el Sr. AA ya ha tenido acceso a toda su información personal pues la misma está contenida en diversos expedientes a los cuales ha tenido acceso, en el marco de lo previsto en el Decreto 500/91 (arts. 12 y 77 de dicho decreto).

Considera ASSE que no aplicaría al caso la Ley N° 18.331, pues el art. 14 habilita al titular a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o

privadas. En el caso, según ellos aprecian, no existiría una base de datos sino un conjunto de expedientes con el objeto de que el Departamento de Certificaciones Médicas de ASSE, pueda determinar la aptitud física y mental del funcionario.

Agrega que tal criterio ha sido sostenido por la Unidad en la citada Resolución N° 93/2013.

Advierten que el solicitante expresa el deseo de acceder a "toda la documentación en poder del departamento de certificaciones médicas relativas a mi persona", y que ello constituye una vaguedad que no puede presuponer la existencia de una base de datos, ni demandar la aplicación de los exiguos plazos del art. 14 de la Ley N° 18.331.

II.- Marco jurídico de análisis

No compartimos gran parte de las apreciaciones formuladas por ASSE, pues consideramos que la ley N° 18.331/2008, consagra un sistema de protección específico para el derecho a la protección de datos (art.1° de la Ley y art. 72 de la Constitución), del cual se desprenden a su vez, un conjunto de derechos y obligaciones con diferente alcance y naturaleza jurídica (arts. 14, 15 y 16).

De ese conjunto de derechos consagrados en la norma, se desprende a su vez la posibilidad de ejercer una Acción de Habeas Data ante la justicia competente por parte del titular de datos personales que considere que sus derechos no han sido garantizados (art. 37).

Actualmente existen diversidad de opiniones respecto a la naturaleza jurídica de la Acción de Habeas Data, que para algunos es un derecho, para otros una garantía, para otros una herramienta procesal destinada a hacer efectivo el ejercicio de los derechos (acceso, rectificación, actualización, inclusión o supresión); hasta llegar a quienes consideran que se trata de ambos (derecho y garantía), o a quienes estiman que se estaría en presencia de un derecho humano de tercera generación.

En definitiva, es claro que corresponde diferenciar o distinguir este haz de derechos y obligaciones que se consagran en la Ley 18.331, respecto de similares derechos y obligaciones que surgen de la normativa que se aplica al ámbito administrativo, especialmente del Decreto 500/91.

Por otra parte, también hay que considerar que, en el ámbito de la salud existe una profusa normativa específica, que alcanza a ASSE y garantiza derechos a los usuarios y pacientes del sistema. En este caso nos referiremos concretamente a la Ley N° 18.335.

III.- Sobre el Derecho de Acceso (art. 14)

En el art. 4 D) de la Ley se establece que dato personal es la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.

Por su parte, en el art. 14 se consagra el derecho a todo titular de datos personales, que previamente acredite su identificación con el documento de identidad o poder respectivo, a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas.

Agrega que tal información debe ser proporcionada dentro de los cinco días hábiles de haber sido solicitada y que vencido el plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas de acuerdo con esta ley, quedará habilitada la acción de habeas data. Se trata pues de un derecho que es tutelable por diversas vías normativas: constitucional, judicial y administrativa.

También se indica que la información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen, que además debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aún cuando el requerimiento sólo comprenda un aspecto de los datos personales.

Creemos que es prístina la norma en cuanto a indicar el alcance que tiene el derecho, por ende sólo por la pertinencia al caso remarcaremos dos aspectos:

- Se extiende a toda la información que se posea acerca del titular, remarcando que "debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aún cuando el requerimiento sólo comprenda un aspecto de los datos personales".
- Se otorga al responsable un plazo de 5 días para entregar dicha información.

Por otra parte, la Ley también tutela otros derechos en los arts. 15 y 16, por lo cual el derecho de acceso claramente es el presupuesto necesario o garantía para el ejercicio de estos otros derechos, pues al conocer o tener acceso a la información personal que se guarda sobre el titular, eventualmente éste también puede rectificar o modificar o impugnar si ello correspondiere.

En este sentido además, en los arts. 37 y siguientes se otorga al titular el derecho de ejercer una Acción de Habeas Data, o Acción de Protección de Datos Personales ante la justicia.

Se agrega que cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso.

En conclusión, es cierto que el Decreto 500/91 determina las reglas para el acceso a los expedientes administrativos, pero este acceso es diferente al derecho de acceso que se consagra en el art. 14, básicamente por dos razones:

a) Su alcance, ya que se circunscribe al contenido específico de un expediente determinado y,

b) La finalidad, que consiste en permitir la correcta defensa en el marco de una actuación administrativa que se ha iniciado contra su persona a raíz del vínculo funcional que se mantiene con la administración, o sea para garantizar el debido proceso en este ámbito.

En cambio, el alcance y la finalidad del derecho de acceso consagrado en el art. 14 de la Ley son claramente otros. Es parte de un derecho humano consagrado en el art 1° de la norma, que se sustenta o se extrae del art. 72 de nuestra Constitución y su finalidad es proporcionar al individuo el derecho a ejercer el control de sus datos personales.

En definitiva, en el caso, -atendiendo al alcance y naturaleza de este derecho e independientemente de que AA acceda o haya accedido al contenido de los expedientes en el marco del Decreto 500/91-, corresponde que ASSE le proporcione en el plazo de 5 días, el acceso a toda otra información que posea y se relacione con él, a modo de ejemplo:

- Listado de los expedientes que se hayan iniciado o se tramiten contra él en esta dependencia de ASSE. (no se trata del contenido de cada uno sino a un listado de los mismos).
- Documentación de diversa índole como minutas, certificaciones o informes de cualquier tipo que no estén contenidos en dichos expedientes
-Toda otra información, ya sea en soporte escrito, informático, imágenes, etc, que se relacione con su persona y se encuentre en la base de datos de pacientes o usuarios que posee esta dependencia de ASSE.

En este sentido, el art. 36 del decreto 500/91 habilita la posibilidad de que no siempre se deba armar un expediente en el ámbito público, o sea que perfectamente pueden existir cartas, memorándum, circulares, formularios, que no formen parte de un expediente (sin perjuicio de que puedan estar agregados a los mismos también), y se relacionen con el denunciante.

En cuanto al acceso a la historia clínica, considera esta informante que atendiendo a la existencia de una norma específica, corresponde que el denunciante la solicite mediante el mecanismo consagrado en el Ley N° 18.335 art. 18 Literal D y art. 33 del Decreto N° 274/2010

IV.- Sobre la existencia o no de una base de datos

Respecto a que no aplicaría al caso el art. 14, pues en el se habla de información que se halle en bases de datos públicas o privadas, y además el solicitante expresa el deseo de acceder a “toda la documentación”, lo cual constituye una vaguedad que no puede presuponer la

existencia de una base de datos, ni demandar la aplicación de los exiguos plazos del artículo, no se comparte tal afirmación, así como tampoco se comparte que la URCDP ya se ha expresado en este sentido en la Resolución N° 93/2013.

Primero porque dicha resolución ha recaído en un caso de denuncia totalmente diferente, donde el denunciante alega que se incluyó en un expediente administrativo público un informe psiquiátrico que lo perjudica y revela datos sensibles.

Segundo porque lo que se expresa en dicha Resolución no es eso. Véase que el primer considerando expresa lo contrario: "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, aunque se considere que el expediente en sí no constituya una base de datos". O sea que, en definitiva la URCDP establece que se aplica la Ley, aunque un sólo expediente en sí mismo no pueda considerarse una base de datos en el sentido establecido en la Ley, pero sí corresponde tener presente que contiene datos personales que deben ser protegidos (información confidencial).

Además, la Ley se aplica al tratamiento de datos "registrados en cualquier soporte" (art. 3° ámbito objetivo), por ello no necesariamente debe presuponerse la existencia de una base de datos como un conjunto organizado de datos, para garantizar y proteger el derecho que consagra la norma.

Asimismo, el dato personal está definido en la norma como la información de cualquier tipo (art. 4). Esta posición es la misma que sostiene el informante en el expediente de referencia N° 2012-2-10-…, Dr. CC, en el informe jurídico que luce a Folio N° 69, antecedente de la mencionada resolución.

En todo caso, se puede hablar de bases de datos excluidas del ámbito de aplicación de la Ley pero en ese caso, debería aplicarse el art. 3° c), y serán bases creadas y reguladas por leyes especiales. En este caso la URCDP se ha expresado al respecto, indicando que cada Organismo público deberá proceder a la inscripción de sus bases de datos dentro del plazo establecido por el Decreto N° 414/009 de 31 de agosto de 2009 (Dictamen N° 17/009), y sólo quedan exonerados aquellos que tengan una regulación legal muy similar a la Ley N° 18..331, a criterio de la URCDP.

V.- Conclusiones

1. La Ley N° 18.331 aplica al caso y alcanza a ASSE y sus dependencias, por ende está obligado a garantizar el derecho de acceso del denunciante dentro del plazo establecido en el art. 14.

2. En razón de lo anteriormente expuesto, corresponde concluir que ASSE ha vulnerado la norma en el caso analizado y por ello se sugiere la aplicación de una sanción de observación (la más baja de acuerdo a la Resolución de la N° 320/009 de la URCDP), considerando que no hay antecedentes para este organismo.
3. Por otra parte, según el informe que luce a Folio N° 72, ASSE no se ha presentado a inscribir sus bases de datos, por ende corresponde que la URCDP también intime a cumplir con lo establecido en el art. 6° de la Ley.

Firmado:
Dra. Graciela Romero
Derechos Ciudadano

Informe Nº 36 BIS, de 26 de marzo de 2014.

Se informa consulta del Colegio Médico del Uruguay acerca de la solicitud de información formulada al Fondo de Solidaridad.

INFORME Nº		EXPEDIENTE Nº
36BIS	2014	2013-2-10-0000097

Montevideo, 26 de marzo de 2014

I.- Introducción

La consulta proviene del Colegio Médico del Uruguay (en adelante CMU), y refiere a la posibilidad de que el Fondo de Solidaridad les comunique el listado de los médicos en actividad, con el fin de actualizar la base de datos que poseen para cumplir con sus cometidos legales.

Se aclara que el CMU es una persona pública no estatal creada por ley N° 18.591 de 18 de setiembre de 2009, que determina su competencia y cometidos.

II.- Análisis del marco legal que aplica

La Ley N° 18.591 crea al CMU "como persona jurídica pública no estatal, con el cometido de garantizar al médico y a la comunidad, el ejercicio de la profesión dentro del marco deontológico establecido".

A su vez, en el art 2º, establece la obligatoriedad de la inscripción en sus registros, pues para "ejercer la profesión de médico en el territorio nacional, se requerirá la vigencia de la inscripción en el registro de títulos del Colegio Médico del Uruguay".

En tanto en la reglamentación de la misma, Decreto N° 83/010, art. 5°, se establece que el CMU llevará un único Registro de Títulos a nivel nacional, que será administrado por el Consejo Nacional y por los Consejos Regionales dentro de su área territorial".

Reitera en el art. 6°, que "ningún médico podrá ejercer su profesión dentro del territorio nacional, si no se encuentra su título inscripto en el Registro referido en el Artículo anterior, o si la inscripción no se encuentra vigente".

Surge entonces que el CMU es un organismo público no estatal, creado por Ley con determinados cometidos y obligaciones, y justamente para cumplir con las mismas, es que debe mantener un registro actualizado de los médicos habilitados para el ejercicio de la profesión en todo el territorio nacional.

La consulta refiere a la posibilidad de que el Fondo de Solidaridad le comunique los datos de

los médicos que egresan, a efectos de actualizar el registro. Manifiestan que el MSP comunica esa información, pero su base de datos no está debidamente depurada (de jubilados o fallecidos) o sea no está actualizada, y es por ello que requieren de la colaboración del Fondo.

No obstante ello, la obligación de mantener un registro actualizado es atribuida por la Ley N° 18.591 al CMU que es quien formula la consulta. No se trata de una obligación legal atribuida a quien va a realizar la comunicación de datos, que en el caso sería el Fondo de Solidaridad, por ello no aplicaría la hipótesis prevista en el art. 9 B) de la Ley.

En cambio, resulta de interés de los profesionales médicos, y a su vez constituye una obligación, el estar inscriptos en dicho registro para poder ejercer, según lo dispuesto por el art. 2 de la Ley N° 18.591. Por ende correspondería aplicar la excepción prevista en el art. 9 D): no se requiere solicitar el consentimiento pues la inscripción en dicho registro hace a la relación profesional ya que la norma establece la obligatoriedad de la inscripción para ejercer la profesión de médico en el territorio nacional.

A pesar de lo anteriormente mencionado, también el art. 17 de la Ley N° 18.331, referido a la comunicación de datos específicamente, establece que los datos objeto de tratamiento podrán ser comunicados sin previo consentimiento, cuando así lo disponga una ley de interés general o en los supuestos del art. 9°. En dicha comunicación debe identificarse un interés legítimo, tanto de quien comunica los datos como del titular de los mismos, cuestión que en el caso se verifica.

En definitiva, aunque opere una comunicación de datos personales que involucra al Fondo de Solidaridad, -excepcionado de recabar el consentimiento de los médicos como ya se analizó-, también se trata de un intercambio de información que incluye datos personales, por ello debe considerarse lo previsto en los arts. 157 a 160 de la Ley N° 18. 719 de 27 de diciembre de 2010, sobre intercambio de información entre Entidades Públicas, estatales o no, así como su decreto reglamentario N° 178/013.

III. Esquema de funcionamiento y formalidades para el intercambio

Sobre el esquema de funcionamiento se debe estar a lo dispuesto en los arts. 5° y siguientes del Decreto 178/013, atendiendo a la finalidad de los datos que se intercambian y al mandato legal existente.

Por otra parte, deberá garantizarse la seguridad de la información que se comunica, mediante trámites y servicios electrónicos que proporcionen niveles adecuados de confidencialidad, integridad y disponibilidad.

En este sentido, el CMU y el Fondo de Solidaridad deberán optar entre celebrar un acuerdo de intercambio de información donde consten las condiciones, mecanismos y responsabilidades de cada uno; o de lo contrario adoptar uno de los mecanismos o condiciones definidas por la AGESIC y formalizar un acuerdo en base a ello.

La Ley N° 18.719 (art. 159), establece además que en ambos casos, el procedimiento se iniciará con la presentación de una solicitud fundada y firmada por el jerarca del organismo que pide información, ante el jerarca del organismo receptor de dicha solicitud, y el acuerdo deberá establecer las condiciones, protocolos y criterios funcionales o técnicos que aplican al intercambio.

Por otra parte, una vez que el acuerdo se celebre, deberá ser inscripto en el Registro de Acuerdos de Interoperabilidad, que llevará a tales efectos AGESIC (art. 160 Ley N° 18.719), dentro del plazo de 90 días a contar desde la firma..

IV. Conclusiones

Al caso resultan aplicables el inciso D) del artículo 9° y el art. 17 de la Ley N° 18.331 que eximen al Fondo de Solidaridad de recabar el previo consentimiento informado de los titulares de los datos, a efectos de ser comunicados.

No obstante, como la consulta no ha sido formulada por el Fondo de Solidaridad, sino por quien requiere de tal comunicación, se debe aplicar también lo dispuesto por los arts. 156 a 160 de la Ley N° 18.719, que indica que se debe formalizar un acuerdo de intercambio de información con las condiciones y requisitos ya mencionados.

Firmado:

Dra. Graciela Romero
Derechos Ciudadanos

Informe Nº 53, de 28 de marzo de 2014.

Se informa consulta presentada por el Programa Salud.uy sobre el componente de teleimagenología.

INFORME Nº		EXPEDIENTE Nº
53	2014	2013-2-10-0000100

Montevideo, 28 de marzo de 2014

I. Antecedentes

El 17 de marzo de 2014 el Director del Programa Salud.uy, Ing. Jorge Forcella, presenta una consulta relacionada con la legitimidad del tratamiento de datos de salud, en el marco del Componente de Teleimagenología. Agrega documentación y gráficas que ilustran el escenario en que se desarrollará el Piloto de la Red Integrada de Servicios de Imagenología, así como las consultas que se formulen.

Pregunta básicamente si es legítima o no la recolección y el tratamiento de datos de salud, -considerados datos sensibles-, en el marco de la implementación y funcionamiento de dicho componente.

Se explica que incluye un Sistema de Información Radiológico, con una arquitectura que permite complementar servicios entre los centros de diagnóstico. Los informes técnicos además, se podrán realizar en forma remota, ya sea en otro centro o por médicos especialistas actuando individualmente.

Para el almacenamiento de las imágenes y diversas tareas de gestión, la solución también contendrá un PACS centralizado.

El nuevo Sistema Nacional de teleimagenología también ofrecerá una plataforma de alcance general (público y privado), para la complementación de servicios en el área, a nivel de todo el país.

Se acota además, que las comunicaciones hacia el PACS y el Sistema de Información Radiológica (RIS), así como las intra institucionales se realizarán sobre un canal seguro que es la RedUY, en tanto, las comunicaciones en el centro de radiología se hacen en una red local aislada de forma lógica del resto de la institución, y las bases de datos residen en servidores independientes y exclusivos para las tareas de imagenología.

En tanto, los datos que visualizan los técnicos y médicos serían: CI, nombres y apellidos, fecha de nacimiento y sexo. Las imágenes generadas en el tomógrafo son visualizadas por un médico radiólogo o un técnico radiólogo en un dispositivo Dicom (estándar reconocido a nivel mundial para el intercambio de pruebas médicas). En estas imágenes se incluyen los datos identificatorios de los pacientes.

II. Marco legal a considerar

Para responder es pertinente considerar todo el marco legal, comenzando por aquel que reconoce a la salud como un derecho fundamental.

Efectivamente, diversos tratados Internacionales de DD.HH aluden a su alcance e importancia como derecho humano a garantizar. Tanto el Protocolo Adicional a la Convención Americana sobre Derechos Humanos, como el Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC), entienden que el derecho a la salud comprende el "disfrute del más alto nivel de bienestar físico, mental y social".

Por otra parte, según el Comité de los Derechos Económicos de la ONU (Comité de vigilancia del PIDESC), es casi imposible para los Estados "garantizar la buena salud o brindar protección contra todas las causas posibles de la mala salud del ser humano (…), por lo tanto, el derecho a la salud debe entenderse como un derecho al disfrute de toda una gama de facilidades, bienes, servicios y condiciones necesarios para alcanzar el más alto nivel posible de salud."
En definitiva, se trata del derecho de las personas a acceder a todos los servicios, facilidades, bienes, etc, disponibles para alcanzar el mejor nivel de salud posible. Esta consideración aplica al caso y es relevante, pues el sistema que se proyecta implementar implica beneficios para los pacientes y usuarios del sistema, resultado del avance de la ciencia y la tecnología aplicados a la mejora de los servicios de salud. [17]

III. Sobre la legitimidad del tratamiento de datos de salud

En lo que respecta al derecho a la protección de datos personales concretamente, según el art. 4° de la Ley N° 18. 331, los datos de salud se deben considerar datos sensibles, y por ello el art. 18 establece que "ninguna persona puede ser obligada a proporcionar datos sensibles", haciendo la salvedad de que "estos podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular".

17. Observación general Nº 14 (2000). El derecho al disfrute del más alto nivel posible de salud (artículo 12 del Pacto Internacional de Derechos Económicos, Sociales y Culturales).COMITÉ DE DERECHOS ECONÓMICOS, SOCIALES Y CULTURALES. 22º período de sesiones. Ginebra, 25 de abril a 12 de mayo de 2000.

Agrega además que: “Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares”.

En definitiva, la norma prevé cuatro hipótesis que legitiman el tratamiento de este tipo de datos considerados sensibles y entre las mismas, ubicamos al consentimiento expreso y escrito del titular en primer lugar, así como razones de interés general o mandato legal atribuido a determinado organismo.

El consentimiento del titular enerva cualquier obstáculo y habilita el tratamiento de este tipo de datos, pero a su vez, -cuando estamos en presencia de un plan o proyecto que apunta a mejorar los servicios de salud-, también median razones de interés general en el entendido de que el Estado debe garantizar *el disfrute de toda una gama de facilidades, bienes, servicios y condiciones necesarios para alcanzar el más alto nivel posible de salud.*

En cuanto al mandato legal, no es menor la existencia de un abundante marco legal específico que regula o refiere al sistema de salud en nuestro país, haciendo énfasis en la Ley N° 18.335 y su decreto reglamentario N° 274/010.

En este sentido, volviendo a la Ley N° 18.331, el art. 18 menciona el mandato legal otorgado al organismo, así como el art.19 indica que los establecimientos sanitarios públicos o privados y los profesionales vinculados a la salud, pueden recolectar y tratar datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieran estado bajo tratamiento de aquellos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la misma. (o sea en la Ley N° 18.331).

Por ende, por normativa específica cabe considerar a la Ley 18.335 y su decreto reglamentario, la que precisamente establece, entre otras consideraciones, que toda persona tiene derecho a acceder a una atención integral que comprenda todas aquellas acciones destinadas a la promoción, protección, recuperación, rehabilitación de la salud y cuidados paliativos, así como tiene derecho a recibir una atención en salud de calidad.

Establece además, que todo paciente tiene el derecho a que sus exámenes diagnósticos, estudios de laboratorio y los equipos utilizados para tal fin cuenten con el debido control de calidad.

Por otra parte, los estudios e informes producidos en el escenario descripto en la consulta, también formarían parte de la historia clínica del paciente, que debe ser completa, ya sea

escrita o electrónica, pues es donde figura la evolución de la salud desde el nacimiento hasta la muerte.

En cuanto al consentimiento, también la Ley 18.335 establece que todo procedimiento de atención médica será acordado entre el paciente o su representante -luego de recibir información adecuada, suficiente y continua- y el profesional de salud. El consentimiento informado del paciente a someterse a procedimientos diagnósticos o terapéuticos estará consignado en la historia clínica en forma expresa.

Por ende, desde el punto de vista de la protección de datos personales, considerando especialmente lo establecido en los arts. 9 B), 9 D), 17 y 18 de la Ley N° 18.331, así como lo expresado en los arts. 6°, 7°, 11 y 18 de la Ley N° 18.335, corresponde concluir que es legítima la recolección, el tratamiento y la comunicación de datos, descriptos en la consulta que se ha formulado.

Es claro que, no obstante ello, en el funcionamiento se deberán observar todos los principios que sustentan la Ley N° 18.331: Veracidad, Finalidad, Previo Consentimiento Informado, Seguridad de los Datos, Reserva y Responsabilidad, los derechos y obligaciones indicados en ella, así como lo formulado especialmente en los arts. 18 y 19, respecto al tratamiento de datos sensibles y datos de salud.

El secreto profesional, la confidencialidad y la reserva son elementos claves (art. 19), así como también es clave la seguridad de la información. Por ello cobran especial importancia las medidas de seguridad que se aplicarían a cada proceso.

La propia Ley N° 18.335 indica en su art. 20, que es de responsabilidad de los servicios de salud dotar de seguridad a las historias clínicas electrónicas y determinar las formas y procedimientos de administración y custodia de las claves de acceso y demás técnicas que se usen, por lo cual el Poder Ejecutivo deberá determinar criterios uniformes mínimos obligatorios de las historias clínicas para todos los servicios de salud.

En el sentido de la consulta, la Pauta Nacional de Teleradiología mencionada, -próxima a publicarse por parte del MSP-, es un documento que aporta en el sentido de establecer criterios uniformes que brinden seguridad.

Por último, cabe considerar que si fuere necesario formalizar el intercambio de información entre entidades del ámbito público, se aplicaría la Ley Nº 18.719, de 27 de diciembre de 2010, que brinda un marco legal acorde y establece garantías para las partes.

Respecto a si es conveniente o no, mediante algún componente informático, anonimizar la información personal, en principio se considera que no. Creemos que identificar correctamente en todas las etapas los informes, imágenes o estudios de una persona, redunda en la calidad de la información y beneficia también a los pacientes en el entendido de que, el hecho de estar asociados a su nombre, es una garantía más de que los mismos efectivamente le pertenecen.

Cuando la Ley N° 18.331, en el art. 17 C) o en el art. 18 refiere a esta posibilidad, comprende otras hipótesis de tratamiento de datos de salud. En el primer caso se trataría de emergencias sanitarias, por ejemplo cuando debe anunciarse públicamente algún tipo de epidemia o enfermedad, etc. Menciona el artículo además, que el mecanismo de disociación debe ser empleado “cuando ello sea pertinente”.

En el segundo caso, el art. 18 refiere a las hipótesis de cuando se tratan datos personales de los pacientes o usuarios “con finalidades estadísticas o científicas”, por ejemplo, en un congreso médico se presenta una investigación determinada o cuando el Ministerio elabora estadísticas para difundir entre la población, etc.

III. Conclusiones

En razón del análisis realizado, cabe responder que la recolección, comunicación y tratamiento de datos personales realizado en el escenario descripto en la consulta, es en principio, respetuoso de la normativa de protección de datos personales.

No obstante ello, por tratarse de datos de salud siempre deberán observarse estrictamente los principios rectores y demás obligaciones previstos en las normas mencionadas, haciendo especial hincapié en la seguridad de la información, sin llegar a considerar esta informante que debe ser necesario y conveniente, en ninguna de las etapas, la disociación de los datos de los titulares.

Firmado:

Dra. Graciela Romero
Derechos Ciudadanos

Informe Nº 158, de 15 de agosto de 2014.

Se informa denuncia sobre comunicación de datos sin consentimiento.

INFORME Nº		EXPEDIENTE Nº
158	2014	2013-2-10-0000231

Montevideo, 15 de agosto de 2014

I. Antecedentes

El 25 de mayo de 2014 la Sra. AA, presenta denuncia contra la Intendencia de Montevideo porque se han comunicado sus datos personales al funcionario que ella ha denunciado por malos tratos ante el Buzón Ciudadano. Indica que con dicha información (incluido el celular y su domicilio), éste llamó a su casa para amenazarla.

Adjunta video de su presentación del caso en el programa de televisión "BB".

Se le otorga vista a la Intendencia que expresa que, a su entender no existe violación a la Ley N° 18.331, no obstante ello dispuso la instrucción de una investigación administrativa según Resolución N° 379/14/5000 de 8 de mayo de 2014, dictada por la Dirección General del Departamento de Gestión Humana y Recursos Materiales.

II. Análisis de la denuncia

Del audio del programa, cuyo texto y constatación notarial lucen agregados al expediente, surge que *"cuando uno hace contacto con el buzón ciudadano se le piden sus datos personales, nombre completo, cédula de identidad, dirección, teléfono y mail. Dependiendo del contenido de la queja el buzón ciudadano lo enviaría a la dependencia correspondiente para luego responder y trasladarle la respuesta a la persona denunciante. Se habla entonces de una base de datos importante que se nutre de la información de todas las personas que contactan con este buzón".*

La denunciante indica en el programa que *"a la semana, el jueves, me llama por teléfono me dice ´señora AA (...) no, no, por que usted se quejó de que yo la traté mal, (...) me van a suspender por su culpa´ le digo y usted (...) en seguida asocié, usted tiene mis datos? dice ´si, si, usted es AA, vive en la calle tal, su cédula de identidad es tal, tengo todos sus datos´"*

Agrega que, el día lunes la llama la directora del buzón ciudadano que quería saber *"si era el tipo el que me había llamado".* La señora AA también relata la existencia de una segunda llamada, por parte de un abogado de la IM que la quería invitar a declarar porque estaban iniciando un sumario a ese funcionario.

En tanto, el Gerente Interino de Servicios de Apoyo de la IM, Ing. Jorge Iriziti, entrevistado por el periodista, expresa que la información del buzón es vista por los funcionarios del servicio y del área a donde corresponde derivar la queja. Agrega que consultó a jurídica y ahí le

indicaron que no es información secreta porque en algún momento al funcionario denunciado hay que darle vista.

CC desconoce quien llamó a la denunciante identificándose como del área sumarios de la IM. Se pregunta quién era ese abogado, *"porque el caso todavía no llegó a jurídica".*

Cabe agregar que al acceder al formulario del Buzón Ciudadano, tanto durante el llenado así como al finalizar la recolección de los datos, la IM no informa a los usuarios acerca de la existencia de la base de datos, del responsable, la finalidad y el ejercicio de su derechos, tal como se establece en el art. 13 de la Ley N° 18.331.

La base de datos que se forma a partir de estos formularios llenados por los interesados tampoco se encuentra inscripta en el Registro de la URCDP, en cumplimiento de lo dispuesto por el art. 6° de la Ley N° 18.331.

a) Finalidad y tratamiento de datos en el procedimiento administrativo

Respecto a que la información en sí no es secreta, corresponde considerar que si bien no lo sería, de acuerdo con la clasificación establecida por la Ley N° 18.381 de Acceso a la Información Pública, el formulario sí contiene datos personales que deben ser tratados como información confidencial a efectos de su correcto procesamiento (art. 10° Ley N° 18.381).

También hay que tener presente que se está en un ámbito público pero reservado en principio, pues la queja implica denunciar a un funcionario en el cumplimiento de sus funciones, por ende si bien es razonable que la información circule, ello debe ser sólo entre quienes deben intervenir y siempre que la finalidad sea investigar y darle trámite a la queja (principio de finalidad).

El art. D. 49 del Capítulo III del Digesto Municipal, precisamente indica que los funcionarios están *"obligados a las más estricta reserva y al secreto profesional en su caso, con relación a terceros, por los actos en los cuales, personal o directamente deben intervenir por razón del cargo. Entre los terceros, inclúyese a las autoridades que no sean los superiores jerárquicos del obligado, a menos que por decisión funcional competente sean relevados de tal obligación".*

Esto quiere decir entonces que, si bien el funcionario tiene derecho a conocer la queja, a que le den vista, a controlar la prueba, a articular su defensa, etc., todo ello debe estar dentro de las formalidades establecidas en las normas, las cuales no habilitan la entrega de la información personal de la denunciante, como el teléfono de su casa o su celular, ni habilitan a los funcionarios a realizar gestiones personales por fuera del expediente o el trámite oficial.

En este sentido, el Artículo D.54 del Capítulo III del Digesto Municipal indica que *"Los funcionarios no podrán tramitar asuntos de terceras personas ante las reparticiones, ni ejercitar ante las mismas ninguna actividad ajena a las funciones que desempeñan, en la forma y condiciones que establece la reglamentación".*

b) Principio de reserva y confidencialidad

Precisamente sobre la reserva, en el art. 7° de la Ley N° 18.331 (Principio de Veracidad), se establece que la recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones de la Ley.

En el caso, el hecho de que la denunciante llene el formulario de Buzón Ciudadano no significa de modo alguno que haya prestado su consentimiento para que otras personas (y mucho menos el denunciado), accedan a sus datos personales.

Tampoco aplican al caso las excepciones previstas en la Ley, pues no se comunican los datos para cumplir con las funciones propias de los poderes del Estado, así como tampoco existe una obligación legal que habilite a dicho tratamiento.

Por otra parte, se trata claramente de ámbitos públicos donde se exige el deber de confidencialidad y reserva, por lo menos hasta que quede firme la resolución o el sumario correspondiente.

El art. 11 de la Ley N° 18.331 establece en este sentido que, aquellas personas físicas o jurídicas que obtuvieron legítimamente información proveniente de una base de datos, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros.

Agrega que las personas que, por su situación laboral u otra forma de relación con el responsable de la base, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público.

Si bien la Ley habla de base de datos, la obligación o principio de reserva aplica perfectamente a todo tratamiento que se realice de la información que contiene un expediente administrativo, y a la conducta y obligaciones que tienen todos los funcionarios públicos que acceden al mismo, con la particularidad o agravante de que los funcionarios públicos también son alcanzados por otras normas específicas relativas a este tema.

La Ley N° 18.331 establece para la protección de los datos personales un régimen específico, que alcanza a los datos registrados en cualquier soporte susceptibles de ser tratados, así como a toda modalidad de tratamiento ya sea en el ámbito público o privado (art. 3°). El titular de esa información tiene el derecho de controlar quien tiene acceso a su información y qué hace con la misma, salvo las excepciones previstas, y esta es la esencia misma de la legislación vigente en esta materia: *el derecho a proteger y a controlar los datos que me pertenecen* (art.1° y 4° L)

c) Principios de Responsabilidad y de Seguridad

La obligación de proteger la información de carácter personal, es una condición de legalidad del tratamiento de datos personales, e implica el deber del responsable y del encargado del

tratamiento, de llevar a cabo las acciones necesarias para proteger los datos ante los riesgos derivados de su tratamiento (control de acceso, resg).

Si bien es cierto que los documentos y las pruebas, no deberán ser información reservada en el marco de una investigación administrativa, ello no obsta a que no deba confundirse el acceso como condición necesaria para el ejercicio del derecho de defensa, con la comunicación de datos personales que se ha denunciado ante la URCDP, comunicación que se ha hecho sin contar con el consentimiento o una justificación legal que la legitime.

Efectivamente, la entrega de los datos personales de la denunciante a terceros que no deban intervenir, se enmarca en la definición legal de comunicación de datos personales (art. 4 B) y 17 de la Ley).

La existencia de un expediente administrativo no es una razón válida para que los responsables de la información la comuniquen justamente al denunciado, alertándolo y generando riesgos para la denunciante.

En definitiva, la gravedad del hecho radica en que los funcionarios tiene responsabilidades específicas en razón de su investidura, y no les está permitido libremente brindar acceso y comunicar información personal a la que acceden en razón de la situación privilegiada que se ostenta.

Es en razón de ello, que se deben considerar ciertas formalidades o reglas que existen a efectos de tramitar una denuncia o una queja, así como las obligaciones que derivan de los principios de reserva y confidencialidad, principios que deben orientar al intérprete sobre todo a la hora de analizar aquellos casos que versan sobre la protección de datos personales (art. 5° in fine).

III. Conclusiones

En consecuencia y en lo que atañe a los cometidos de la URCDP, se considera que ha existido una vulneración de la Ley N° 18.331, en los arts. 1°, 5°, 6°, 7°, 8°, 9°, 10, 11, 12, 13 y 17. La URCDP deberá aplicar la sanción que estime pertinente considerando que la comuna no tiene antecedentes negativos ante esta Unidad.

Por otra parte, corresponde indicar a la IM que debe inscribir la base de datos que surge del Buzón Ciudadano, así como informar a los interesados que utilicen el servicio en los términos del art. 13 de la Ley, mediante una clausula agregada al pie del formulario u otro medio idóneo.

Atendiendo a la posibilidad de que recaiga una resolución no favorable a los intereses del denunciado, se solicita dar vista previa en los términos de los arts. 75 del Decreto Nº 500/991 de 27 de setiembre de 1991.

Firmado:

Dra. Graciela Romero
Derechos Ciudadanos

Informe Nº 226, de 14 de noviembre de 2014.

Se informa denuncia por comunicación de datos sin consentimiento del titular.

INFORME Nº		EXPEDIENTE Nº
226	2014	2013-2-10-0000270

Montevideo, 14 de noviembre de 2014

I.-

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 la Dirección General de Registro de Estado Civil (DGREC) del Ministerio de Educación y Cultura (MEC).

De la denuncia presentada surge que el denunciante con fecha 4 de junio de 2014 solicitó testimonio de Partida de matrimonio vía web y el organismo al enviarla por correo postal adhirió en el exterior del sobre una etiqueta conteniendo todos los datos personales del Sr. AA (nombre y apellido, fecha de matrimonio, datos de su cónyuge, fecha de matrimonio, número de celular y correo electrónico, y datos del acta de matrimonio).
Manifiesta el denunciante que sucede lo mismo en caso de solicitar testimonio de partidas de nacimiento.

II.-

Se confirió vista a la Dirección General de Registro de Estado Civil, quien expresa que carece de personería jurídica para ser emplazada judicial o administrativamente debiendo entenderse cualquier cuestión directamente con el Ministerio.

Asimismo expresa que resulta imposible que la DGREC vulnere lo dispuesto por la Ley 18.331, por lo previsto en el artículo 2 literal c ya que las bases de datos que maneja fueron creadas y reguladas por la Ley 1.430.

III.-

Atento a que la denuncia involucra otros extremos como el deber de inscripción de las bases de datos de los organismos en cuestión, se confirió vista de igual forma al MEC el 19 de setiembre de 2014, quien a la fecha no compareció.

Corresponde aclarar que la Dirección General de Registro de Estado Civil (DGREC) es la Unidad Ejecutora número 21 del inciso 11, la cual cuenta con sus propios cometidos y facultades por lo que la denuncia debe seguirse adelante con la citada Dirección ya que es quien establece los criterios de actuación operativa y administrativa dentro de la misma.

IV.-

Por otra parte se reitera que la Unidad Reguladora y de Control de Datos Personales (URCDP), es un órgano con la más amplia autonomía técnica, cuya competencia es custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto de sus principios. Por lo tanto si bien la DGREC maneja bases de datos creadas y reguladas por la Ley 1430, por tanto no alcanzadas por la Ley 18.331 por contar con un régimen especial, las Bases de Datos de estado civil que lleva la DGREC no serían inscribibles en el Registro que lleva la URCDP, pero sí hace aplicable todo el régimen tuitivo de la Ley 18.331 de Protección de Datos Personales (PDP) a los datos en ellas contenidos. Por tal motivo, toda base de datos que no refieran a estado civil de las personas, (y que por tanto no se encuentren amparadas por la Ley 1.430) que lleve la DGREC o el MEC, como por ejemplo base de datos de proveedores, funcionarios, videovigilancia, etc. deberán inscribirse ante la URCDP conforme a los artículos 6 y 29 de la Ley 18.331.

Además, si bien la DGREC no debe inscribir los registros de estado civil propiamente dichos, si debe respetar todos los principios contenidos en la Ley de Protección de Datos Personales, por lo tanto no debe exponer datos de un solicitante de testimonios de partidas que requieran consentimiento, en el exterior de un sobre de correo postal, tomando medidas para asegurarlos.

V.-

La denunciada expresa que el "celo del solicitante ahora denunciante no se compadece con la petición de que el envío de la partida se haga a su lugar de trabajo y no a su residencia particular ya que si hubiera procedido de esta última forma ningún eventual agravio le habría causado en tanto nadie extraño habría visualizado el formulario pegado a la carta".

Cabe precisar que los datos fueron entregados con la finalidad específica de obtener el testimonio de una partida, no siendo relevante el lugar donde eligió recibirla ya que de mantenerse el criterio que sostiene la DGREC si una persona se domicilia en una propiedad horizontal sus datos correrían el riesgo de ser visualizados por los copropietarios. Por ende, la DGREC debería extremar los cuidados e incluir en la etiqueta adherida al sobre solo los datos mínimos necesarios para efectuar la entrega del testimonio de la Partida a saber, nombre y dirección de entrega seleccionada por el solicitante.

Conclusiones

1.- Atento a lo expresado, corresponde señalar que la DGREC en aplicación de los principios rectores en materia de Protección de Datos Personales, deberá extremar las medidas para preservar y asegurar los datos entregados por los particulares al solicitar testimonios de partidas, aun cuando no sean incluidos en una base de datos de solicitudes o similar y reducir al mínimo los datos a incluir en la etiqueta adherida al sobre de correo postal.

2.- Se aconseja intimar la inscripción de las bases de datos (funcionarios, proveedores, videovigilancia, etc.) de las que sean responsables el Ministerio de Educación y Cultura y a la Dirección General de Registro de Estado Civil en un plazo de 30 días corridos, bajo apercibimiento.

Es todo cuanto tengo que informar.

Firmado:

Dra. María Cecilia Montaña Charle
Derechos Ciudadanos

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

agesic
agencia de gobierno electrónico
y sociedad de la información

PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY