



BICENTENARIO.UY
INSTRUCCIONES
DEL AÑO XIII



agesic

agencia de gobierno electrónico
y sociedad de la información



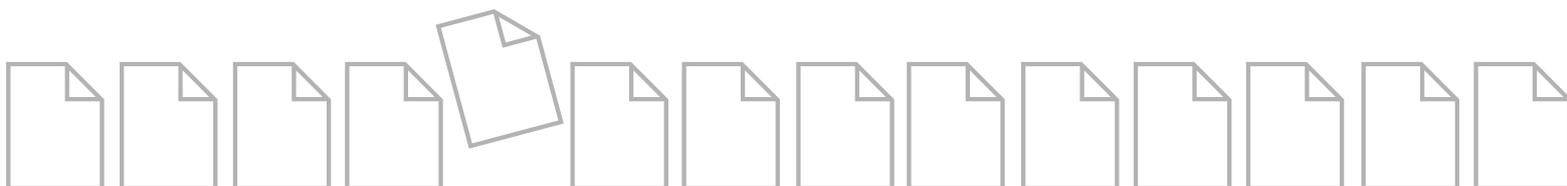
UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

20
12

Resoluciones
Dictámenes
e Informes



20 | Resoluciones 12 | Dictámenes e Informes



Índice de Resoluciones, Dictámenes e Informes

Resoluciones

PAG.

- 12..... **Resolución N° 34A/2012**, de 9 de marzo de 2012. Se resuelve sobre la denuncia presentada contra empresa por utilizar el número telefónico del denunciante para realizar promociones, sin su consentimiento.
- 13..... **Resolución N° 135/2012**, de 2 de marzo de 2012. Se resuelve sobre los recursos administrativos de revocación y jerárquico en subsidio presentados contra la Resolución N° 1658/2011 referida a denuncia contra una entidad pública por mantener información de sanciones a profesionales en su sitio web.
- 14..... **Resolución N° 136/2012**, de 2 de marzo de 2012. Se resuelve sobre solicitud del denunciante de dejar sin efecto la Resolución N° 1178/2011 que resuelve sobre denuncia presentada por el acceso que tuvieron dos funcionarios del gremio, a su expediente de solicitud de subsidio por desempleo.
- 15..... **Resolución N° 137/2012**, de 2 de marzo de 2012. Se resuelve sobre la denuncia presentada contra una empresa por anotaciones que figuran en su base de datos e impiden la gestión de un préstamo.
- 17..... **Resolución N° 142/2012**, de 5 de marzo de 2012. se resuelve sobre la denuncia presentada contra dos empresas por utilizar una base de datos con la finalidad de acosar moralmente al familiar de un deudor.
- 18..... **Resolución N° 172/2012**, de 15 de marzo de 2012. Se resuelve sobre un Código de Conducta para el Funcionamiento de la Base Positiva y el Anexo referente a la Categoría de Datos a incluir en la base de datos respectiva, por parte de empresa que brinda información de carácter objetivo.
- 20..... **Resolución N° 257/2012**, de 29 de marzo de 2012. Se resuelve sobre la regularidad jurídica de la instrucción banco centrista N° 2011/0135, pidiendo que se ordene el retiro de cierta información que figuraba en un blog accesible vía internet.
- 21..... **Resolución N° 258/2012**, de 29 de marzo de 2012. Se resuelve sobre la petición de información en relación con las bases de datos personales de Administración Nacional de Telecomunicaciones (ANTEL) que figuran registradas ante la URCDP.
- 22..... **Resolución N° 285/2012**, de 12 de abril de 2012. Se resuelve sobre la denuncia presentada contra dos empresas por realizar llamadas sin consentimiento a efectos de ofrecer tarjetas de crédito.
- 23..... **Resolución N° 286/2012**, de 26 de mayo de 2012. Se resuelve sobre denuncia presentada contra empresa por ofrecimiento de tarjeta de crédito sin consentimiento.
- 24..... **Resolución N° 288/2012**, de 12 de abril de 2012. Se resuelve sobre la denuncia presentada contra una empresa por el envío de correos no solicitados.

PAG.

- 25..... Resolución N° 289/2012**, de 12 de abril de 2012. Se resuelve sobre la denuncia presentada contra una empresa por el tratamiento excesivo de datos personales, ya que el denunciante entiende que no corresponde se solicite copia de la cédula de identidad a los beneficiarios de sus promociones.
- 26..... Resolución N° 301/2012**, de 19 de abril de 2012. Se resuelve sobre la denuncia formulada contra una institución bancaria por realizar un tratamiento del teléfono celular del denunciante sin su consentimiento.
- 27..... Resolución N° 654/2012**, de 5 de julio de 2012. Se resuelve sobre la denuncia presentada contra una empresa pública debido a que se atribuye a la denunciante un contrato que ya ha sido otorgado a otra persona de igual nombre.
- 29..... Resolución N° 674/2012**, de 19 de julio de 2012. Se resuelve sobre la impugnación de Resolución N° 1658/2011 recaída en expediente relativo a la publicación en la web de información sobre sanciones de profesionales por parte de un organismo encargado de la superintendencia y control.
- 30..... Resolución N° 699/2012**, de 9 de agosto de 2012. Se resuelve sobre el informe relativo al artículo 291 del Proyecto de Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al Ejercicio 2011, que refiere a la posibilidad de mantener los datos inscriptos en la Central de Riesgos, una vez vencidos los plazos correspondientes.
- 32..... Resolución N° 700/2012**, de 9 de agosto de 2012. Se resuelve sobre el informe relativo al artículo 264 del Proyecto de Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al ejercicio 2011, que refiere a la ampliación de las facultades otorgadas a la Dirección General Impositiva (DGI) respecto de lo que no registrarán las limitaciones establecidas en la Ley N° 18.331 de Protección de Datos Personales.
- 35..... Resolución N° 810/2012**, de 6 de setiembre de 2012. Se resuelve sobre la denuncia presentada contra una empresa por incluir en la guía telefónica nombre y teléfono del denunciante sin su consentimiento.
- 36..... Resolución N° 811/2012**, de 6 de setiembre de 2012. Se resuelve sobre la denuncia presentada contra una institución bancaria por el envío de una tarjeta de crédito promocional, expedida por una compañía de telefonía de la cual el denunciante no es cliente.
- 38..... Resolución N° 871/2012**, de 20 de setiembre de 2012. Se resuelve sobre la denuncia presentada contra una empresa por el envío de correos electrónicos sin el consentimiento correspondiente.
- 39..... Resolución N° 931/2012**, de 18 de octubre de 2012. Se resuelve sobre la denuncia presentada contra editor de un periódico barrial, por utilizar sin el consentimiento los nombres e información relacionada con funcionarios de un complejo de viviendas.
- 40..... Resolución N° 982/2012**, de 15 de noviembre de 2012. Se resuelve denuncia en la cual se alega no haber logrado en tiempo y forma la eliminación de datos personales en una base de datos utilizada para promoción de servicios de parte de la institución bancaria denunciada.

PAG.

- 41..... Resolución N° 1034/2012**, de 13 de diciembre de 2012. Se resuelve sobre denuncia presentada contra una institución pública educativa por el uso de imágenes tomadas por las cámaras de videovigilancia como prueba en un procedimiento sumarial.
- 42..... Resolución N° 1035/2012**, de 13 de diciembre de 2012. Se resuelve sobre denuncia presentada contra una institución pública educativa por la existencia de bases de datos que no se encuentran inscriptas.
- 43..... Resolución N° 1036/2012**, de 13 de diciembre de 2012. Se resuelve sobre denuncia presentada contra una institución bancaria por el envío de una tarjeta de crédito sin el consentimiento correspondiente.
- 44..... Resolución N° 1040/2012**, del 20 de diciembre de 2012. Se resuelve sobre el informe técnico brindado por el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), respecto a las posibilidades que brinda la tecnología para evitar que ciertos contenidos sean indexados e incluidos en el caché de los buscadores de internet, a efectos de garantizar la protección de datos personales y en especial el derecho al olvido.
- 46..... Resolución N° 1041/2012**, de 20 de diciembre de 2012. Se resuelve sobre la inscripción de un Código de Conducta.
- 47..... Resolución N° 1043/2012**, de 20 de diciembre de 2012. Se resuelve sobre la propuesta de la Secretaría Permanente de la Red Iberoamericana de Protección de Datos, respecto a brindar impulso al Proyecto de Cooperación para el intercambio de información en materia de protección de datos de menores, que permita conocer los recursos disponibles y servicios tecnológicos existentes para enfrentar los riesgos que implica la utilización de las TIC y en especial internet.

Dictámenes

- 50..... Dictamen N° 1**, de 15 de marzo de 2012. Se dictamina en relación con la procedencia de la aplicación de la Ley 18.331 a los objetivos del grupo llamado “Apostasía Colectiva en Uruguay”.
- 51..... Dictamen N° 2**, de 22 de marzo de 2012. Se dictamina en relación con la consulta formulada respecto a la redacción de una cláusula de confidencialidad a ser incorporada en el Fondo Concursable LA 21 de la Dirección Nacional de Empleo.
- 52..... Dictamen N° 3**, de 29 de marzo de 2012. Se dictamina en relación con la consulta formulada acerca de la existencia de la obligación de registrar su base de datos de afiliados, por parte del Centro Integral del Personal de ANTEL (CIPA).
- 53..... Dictamen N° 4**, de 12 de abril de 2012. Se dictamina en relación con la consulta formulada respecto a la celebración de un convenio de intercambio de datos entre la Intendencia de Canelones y Obras Sanitarias del Estado (OSE).

PAG.

- 55..... Dictamen N° 5**, de 13 de abril de 2012. Se resuelve en relación con la consulta referida a la utilización de Identificadores de Objetos (OIDs) en el Ministerio de Relaciones Exteriores para identificar el ingreso de un usuario a la red.
- 57..... Dictamen N° 6**, de 15 de mayo de 2012. Se dictamina en relación con la ampliación de consulta formulada por el Carrasco Lawn Tennis Club, respecto a si resulta ajustada a derecho la entrega de los datos personales que figuran en el padrón social, cuando así lo requieren sus socios.
- 58..... Dictamen N° 7**, de 10 de mayo de 2012. Se dictamina en relación con la consulta realizada por el Banco de Previsión Social (BPS) respecto si es suficiente la solicitud de turno o cita como forma de recabar el consentimiento para acceder a la historia clínica.
- 60..... Dictamen N° 8**, de 15 de mayo de 2012. Se dictamina en relación con la consulta proveniente de la Dirección Nacional de Hidrografía del Ministerio de Transporte y Obras Públicas (MTO), acerca de la adecuación de un sistema informático en desarrollo para la gestión de los puertos con la Ley N° 18.331.
- 61..... Dictamen N° 9**, de 24 de mayo de 2012. Se dictamina en relación con la consulta formulada por un integrante del Comité de Seguridad de la Información de la Agencia Nacional de Vivienda (ANV) respecto a la pertinencia y uso del correo electrónico entregado a los usuarios, así como la regulación de la privacidad de la información contenida en los mismos.
- 63..... Dictamen N° 10**, de 18 de mayo de 2012. Se dictamina en relación con la consulta formulada por la Intendencia de Rocha respecto a la información solicitada por un Edil Departamental con relación a una Casa Refugio que atiende a personas en situación de calle.
- 65..... Dictamen N° 11**, de 31 de mayo de 2012. Se dictamina la consulta formulada por los representantes del Nautilus Yachting sobre la comunicación de los datos del padrón electoral.
- 66..... Dictamen N° 12**, de 7 de junio de 2012. Se dictamina la consulta formulada por la Unidad de Acceso a la Información Pública (UAIP), respecto a la solicitud de información presentada ante la Intendencia de Montevideo y continente de datos personales.
- 68..... Dictamen N° 13**, de 28 de junio de 2012. Se dictamina la consulta formulada respecto al sistema de defunciones digital que se está implementando por parte del Ministerio de Salud Pública (MSP).
- 70..... Dictamen N° 14**, de 28 de junio de 2012. Se dictamina respecto a la consulta formulada por el Instituto Nacional de las Mujeres-Departamento de las Mujeres Afrodescendientes del Ministerio de Desarrollo Social (MIDES), relativa a la formación e inscripción de una base de datos territorial de profesionales y/o técnicos de origen afrodescendientes.

PAG.

- 72..... Dictamen N° 15**, de 2 de agosto de 2012. Se dictamina consulta formulada por el Fondo de Cesantía y Retiro de la Construcción (FOCER) relacionada con la comunicación de información que incluye datos personales de los beneficiarios.
- 74..... Dictamen N° 16**, de 9 de agosto de 2012. Se dictamina la consulta realizada por la Secretaría de la Cámara de Senadores acerca de la adecuación de las versiones taquigráficas de algunas actividades de la Cámara, a la Ley N° 18.331 y su Decreto reglamentario N° 414/009.
- 77..... Dictamen N° 17**, de 16 de agosto de 2012. Se dictamina la consulta presentada por el Ministerio de Educación y Cultura (MEC), Dirección General de Registro de Estado Civil (DGR), respecto a las solicitudes de acceso que recibe de parte de organismos públicos y privados, vinculado con la información contenida en sus bases de datos.
- 79..... Dictamen N° 18**, de 30 de agosto de 2012. Se dictamina la consulta realizada por la Asesoría Letrada de la Dirección General de Registro (DGR) vinculada con la publicación en la página web de las resoluciones administrativas.
- 80..... Dictamen N° 19**, de 6 de setiembre de 2012. Se dictamina la consulta referida a las eventuales consecuencias jurídicas que tendría contratar el servicio de videovigilancia ofrecido por la Administración Nacional de Telecomunicaciones (ANTEL), que permite instalar una cámara en la cocina-comedor del domicilio particular donde cumple funciones una niñera.
- 82..... Dictamen N° 20**, de 6 de setiembre de 2012. Se dictamina la consulta realizada por Nalistar S.A. Vinculada a si corresponde una cláusula en un contrato de adhesión.
- 83..... Dictamen N° 21**, de 20 de setiembre de 2012. Se dictamina la consulta realizada por la Administración de las Obras Sanitarias del Estado (OSE), respecto a si procede comunicar datos de funcionarios y sus cónyuges al Servicio de Garantía de Alquileres de la Contaduría General de la Nación.
- 84..... Dictamen N° 22**, de 4 de octubre de 2012. Se dictamina la consulta formulada por la Secretaría General de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) acerca de la adecuación de determinados aspectos del pliego de licitación del sistema de denuncia en línea del Ministerio del Interior (MI).
- 86..... Dictamen N° 23**, de 4 de octubre de 2012. Se dictamina la consulta realizada por la Dirección de Epidemiología del Ministerio de Salud Pública (MSP) respecto a la regulación de las bases de datos de las cuales es responsable.
- 87..... Dictamen N° 24**, de 4 de octubre de 2012. Se dictamina la consulta formulada por la Unidad de Acceso a la Información Pública (UAIP) respecto al carácter que poseen determinados datos personales que se incluyen en una solicitud de acceso presentada ante el Ministerio de Relaciones Exteriores (MREE).

PAG.

- 89..... Dictamen N° 25**, de 12 de octubre de 2012. Se dictamina la consulta formulada respecto a los casos de interoperabilidad o intercambio de información entre organismos públicos (artículo 157 Ley N° 18.719), que implican comunicación de datos personales y donde aplica la excepción del literal b) del artículo 9° de la Ley N° 18.331.
- 91..... Dictamen N° 26**, de 1 de noviembre de 2012. Se dictamina la consulta vinculada a cómo adecuar el contenido de las resoluciones del Directorio de la Administración de las Obras Sanitarias del Estado (OSE), a lo establecido en la Ley N° 18.331 a efectos de éstas sean publicadas en la web de dicho organismo.
- 93..... Dictamen N° 27**, de 15 de noviembre de 2012. Se dictamina el Proyecto de Ley presentado por los Señores Senadores Francisco Gallinal y Luis Alberto Lacalle (Carpeta N° 978/2012 de la Cámara de Senadores) para modificar la redacción del art. 22 de la Ley N° 18.331.
- 95..... Dictamen N° 28**, de 15 de noviembre de 2012. Se dictamina la consulta formulada por la Intendencia de Paysandú respecto a un eventual convenio de digitalización de documentos a suscribirse con otra entidad.
- 97..... Dictamen N° 29**, de 13 de diciembre de 2012. Se dictamina la consulta relativa a si el Fondo de Solidaridad se encuentra habilitado para obtener cierta clase de datos personales que disponen los organismos tributarios recaudadores, para el mejor cumplimiento de sus cometidos.
- 99..... Dictamen N° 30**, de 13 de diciembre de 2012. Se dictamina respecto a la consulta formulada por la Auditoría Interna de la Nación (AIN) sobre el régimen a aplicar a cierta información que recibe proveniente de la Dirección General Impositiva (DGI).
- 101..... Dictamen N° 31**, de 20 de diciembre de 2012. Se dictamina acerca de la consulta formulada respecto a la legalidad de la comunicación de las imágenes almacenadas en una videocámara a solicitud de terceros.

Informes

- 104..... Informe N° 5**, de 3 de enero de 2012. Se informa sobre la aplicación de la Ley N° 18.331 en cuanto a la Apostasía y el Habeas Data.
- 107..... Informe N° 11**, de 5 de enero de 2012. Se informa sobre la denuncia contra una institución bancaria por recepción de reiteradas llamadas a su celular sin su consentimiento.
- 109..... Informe N° 27**, de 19 de enero de 2012. Se informa sobre la consulta vinculada a la instalación de una cámara de videovigilancia en la cocina-comedor de un particular.
- 114..... Informe N° 64**, de 8 de febrero de 2012. Se informa la consulta sobre una cláusula de confidencialidad a ser incorporada en el marco del Fondo Concursable LA 21.
- 116..... Informe N° 78**, de 8 de febrero de 2012. Se informa la denuncia contra una empresa consultora por el envío de correo electrónico no deseado.

PAG.

- 118..... Informe N° 106**, de 27 de febrero de 2012. Se informa consulta del Ministerio de Relaciones Exteriores sobre utilización de Identificadores de Objetos (OIDs) para identificar usuarios.
- 121..... Informe N° 153**, de 19 de marzo de 2012. Se informa sobre la consulta del Centro Integral del Personal de ANTEL (CIPA) relativo a la obligación de inscribir las bases de datos.
- 123..... Informe N° 201**, de 19 de abril de 2012. Se informa sobre la consulta realizada por Agencia Nacional de Vivienda sobre la pertenencia y el uso del correo electrónico entregado a los usuarios, así como de la regulación de la privacidad de la información contenida en los mismos.
- 128..... Informe N° 209**, de 24 de abril de 2012. Se informa sobre la consulta presentada por Ministerio de Transporte y Obras Públicas (MTO) con relación al uso de datos personales en desarrollo informático.
- 130..... Informe N° 213**, de 25 de abril de 2012. Se informa sobre la consulta realizada por la Intendencia de Rocha vinculada a la comunicación de datos personales de beneficiarios de una casa refugio.
- 133..... Informe N° 265**, de 14 de mayo de 2012. Se informa sobre la consulta acerca del sistema de intercambio de datos de defunciones en sistema digital que actualmente se está implantando en el Ministerio de Salud Pública.
- 137..... Informe N° 277**, de 24 de mayo de 2012. Se informa sobre una consulta vinculada con la adecuación de Resoluciones de la Administración de las Obras Sanitarias del Estado (OSE) a la Ley de Protección de Datos.
- 143..... Informe N° 283**, de 25 de mayo de 2012. Se informa sobre una consulta presentada por INMUJERES-MIDES vinculada con la formación de base de datos de afrodescendientes.
- 148..... Informe N° 271**, de 17 de mayo de 2012. Se informa sobre la denuncia presentada contra una institución bancaria por no proceder a eliminar el correo electrónico del denunciante de la base de datos de marketing.
- 151..... Informe N° 270**, de 18 de mayo de 2012. Se informa sobre la denuncia presentada contra un comercio donde se fue víctima de un hurto, por no facilitar éste la videograbación del local para efectuar la denuncia.
- 152..... Informe N° 318**, de 6 de junio de 2012. Se informa sobre la consulta acerca de la legalidad de la comunicación de datos realizada por parte del Fondo de Cesantía y Retiro de la Construcción (FOCER).
- 155..... Informe N° 336**, de 13 de junio de 2012. Se informa sobre la denuncia contra un organismo público por no corroborar la identidad y otorgar un contrato por error a otra persona de igual nombre.
- 157..... Informe N° 408**, de 22 de junio de 2012. Se informa la consulta acerca de la adecuación con la Ley N° 18.331 del sistema de denuncias en línea del Ministerio del Interior.

PAG.

- 159..... Informe N° 337**, de 13 de julio de 2012. Se informa sobre una consulta del Ministerio de Educación y Cultura, Dirección General de Registro de Estado Civil, vinculado con las solicitudes de datos que recibe de otros organismos públicos o privados.
- 161..... Informe S/N**, de 26 de julio de 2012. Se informa sobre el alcance del artículo 291 del Proyecto de Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal. Ejercicio 2011, que refiere a la posibilidad de mantener los datos inscriptos en la Central de Riesgos, una vez vencidos los plazos correspondientes.
- 165..... Informe N° 391**, de 26 de julio de 2012. Se informa sobre la denuncia contra un periódico barrial por la publicación de datos personales de funcionarios del complejo de viviendas.
- 168..... Informe N° 362**, de 21 de agosto de 2012. Se informa sobre consulta de la Asesoría Letrada de la Dirección General de Registro vinculada con la publicación en la página web de las resoluciones administrativas.
- 170..... Informe N° 430**, de 23 de agosto de 2012. Se informa una consulta presentada por la Asociación de Despachantes de Aduana del Uruguay (ADAU) sobre datos publicados por la Dirección Nacional de Aduanas.
- 175..... Informe N° 414**, de 27 de agosto de 2012. Se informa sobre una consulta del Ministerio de Salud Pública, División Epidemiología, respecto a la aplicación de la Ley N° 18.331 a las bases de datos relativas a la mortalidad, natalidad, información perinatal y enfermedades de notificación obligatoria.
- 180..... Informe N° 428**, de 4 de setiembre de 2012. Se informa sobre un Proyecto de Ley sobre censura previa y derecho de respuesta en redes sociales.
- 185..... Informe N° 481**, de 12 de setiembre de 2012. Se informa sobre el Proyecto de Ley presentado por los Senadores Francisco Gallinal y Luis Alberto Lacalle vinculado a la modificación del art. 22 de la Ley N° 18.331
- 188..... Informe técnico S/N del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)**, relativo a las diferentes soluciones técnicas aplicables para que la información personal pueda ser eliminada de los sitios web de un organismo público.



Resoluciones



Resolución N° 34A/2012, de 9 de marzo de 2012.

Se resuelve sobre denuncia presentada contra empresa por utilizar número telefónico del denunciante para realizar promociones, sin su consentimiento.

| RESOLUCION No. | | EXPEDIENTE No. |
|----------------|------|-------------------|
| 34A | 2012 | 2011-2-10-0000416 |

Montevideo, 9 de marzo de 2012.

VISTO: La denuncia presentada con fecha 28 de junio de 2011 contra AA por utilizar el número telefónico del denunciante para realizar promociones, sin su consentimiento.

RESULTANDO: I) Que con fecha 17 de agosto del corriente, se presenta AA, indicando que el teléfono del denunciante fue proporcionado por BB.

II) Que con fecha 11 de noviembre del corriente se presenta BB, a manifestar que comunicó a AA, nombre, apellido y teléfono proveniente de fuentes públicas de información. Asimismo indica que los datos fueron comunicados con anterioridad a la Resolución N° 1658/2010, que sanciona a BB por cesión de datos.

CONSIDERANDO: I) Que el hecho que los datos personales se hayan obtenido de una fuente accesible al público, no faculta a la denunciada a tratar de forma contraria a la legislación vigente los mismos.

II) Que existe por parte de las empresas la obligación de respetar el principio de finalidad de los datos consagrado en el artículo 8° de la Ley N° 18.331, así como informar sobre sus derechos a las personas incluidas en la base de datos, atento a lo establecido en el artículo N° 14.

III) Que por Resolución N° 423/11 de fecha 24 de marzo del corriente se sancionó a AA con observación, en el expediente N° 2945/2010.

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

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

1. ESTABLECER QUE EXISTIÓ CONTRAVENCIÓN POR PARTE DE LA DENUNCIADA AL PRINCIPIO DE FINALIDAD DE LA LEY N° 18.331, POR LO QUE SE APLICA A DICHA EMPRESA UNA SANCIÓN DE APERCIBIMIENTO.

2. NOTIFÍQUESE Y PUBLÍQUESE.r.i.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 135/2012, de 2 de marzo de 2012.

Se resuelve sobre recursos administrativos de revocación y jerárquico en subsidio presentados contra la Resolución N° 1658/2011 referida a denuncia contra entidad pública por mantener información de sanciones a profesionales en su sitio web.

| RESOLUCION No. | | Expediente No |
|----------------|-----|-------------------|
| 135 | 012 | 2011-2-10-0000079 |

Montevideo, 8 de marzo de 2012.

VISTO Y **CONSIDERANDO**: I) Los recursos administrativos de revocación y jerárquico en subsidio presentados contra la Resolución N° 1658/2011 recaída en el expediente.

II) Que se ha instruido el recurso de revocación y emitido al respecto el informe jurídico N° 114/2012, sin que hasta la fecha la impugnante haya realizado una ampliación de los fundamentos de su escrito, según la reserva indicada en el tercer petitorio de éste.

III) Que reexaminada la situación fáctica del ocurrente, la normativa aplicable y las alegaciones expuestas por la impugnante, no se hará lugar al recurso de revocación interpuesto y se dispondrá elevar el expediente para tramitar el recurso jerárquico subsidiario, compartiéndose totalmente el informe antes indicado, cuyas conclusiones se dan por reproducidas a título de motivación y fundamento del presente acto.

ATENTO: A lo precedentemente expuesto, a lo informado por el Asesor Letrado y a lo dispuesto por los arts. 31 y 34 (en especial el apartado "D") de la Ley N° 18.331, 142 y ss. del Decreto N° 500/991 y normas concordantes,

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

RESUELVE:

1.- No hacer lugar al recurso de revocación interpuesto contra la Resolución N° 1658/2011, de 7 de diciembre de 2012.2.

2.- Notifíquese personalmente a la recurrente, y elévese el expediente a la Presidencia de la República para la sustanciación del recurso jerárquico subsidiariamente interpuesto.

m.b

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 136/2012, de 2 de marzo de 2012.

Se resuelve sobre solicitud del denunciante de dejar sin efecto la Resolución N° 1178/2011 que resuelve sobre denuncia presentada a raíz del acceso que tuvieron dos funcionarios del gremio a su expediente de solicitud de subsidio por desempleo.

| RESOLUCION No. | | Expediente No. | |
|----------------|----|----------------|---------|
| 136 | 12 | 2011-2-10 | 0000142 |

Montevideo, 8 de marzo de 2012.

VISTO: La solicitud del denunciante de dejar sin efecto la Resolución N° 1178/2011.

RESULTANDO: I) Que el Informe N° 6337/2011 estimó que no existió infracción en la especie denunciada, sugiriendo el archivo de la causa.

II) Que el Consejo entendió que el denunciante ya había expresado todos sus argumentos y fundamentos en defensa de su postura, a través del escrito obrante a folios 95 a 105.

III) Que el denunciante se alza contra dicho parecer, requiriendo se le conceda la oportunidad de controvertir el Informe N° 6337/2011 y ofrecer nuevas pruebas si lo considerase conveniente, antes de resolver el caso.

CONSIDERANDO: I) Que de conformidad con lo solicitado, y al tenor de lo sugerido por el informante de folios 136 (rectius cuando alude a la Res. N° 1173/2011 debe entenderse hecha tal referencia a la Res. N° 1178/2011), se hará lugar a la petición o recurso formulado.

II) Que con ello no se prejuzga sobre el resultado final de estos obrados, permitiendo satisfacer, no obstante, un reclamo del administrado que va en loable línea de aumentar las garantías del debido proceso administrativo.

ATENTO: Al Informe de folios 136, y al art. 75 del Decreto N° 500/991,

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

RESUELVE:

Dejar sin efecto la Resolución N° 1178/2011, y en su lugar confiérase ulterior vista del Informe N° 6337/2011 al peticionante-recurrente.

m.b.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 137/2012, de 2 de marzo de 2012.

Se resuelve sobre denuncia presentada contra empresa por anotaciones que figuran en su base de datos e impiden la gestión de un préstamo.

| RESOLUCION N° | | EXPEDIENTE N° |
|---------------|------|-------------------|
| 137 | 2012 | 2011-2-10-0000316 |

Montevideo, 2 de marzo de 2012.

VISTO: La denuncia presentada el 9 de febrero de 2011 contra AA, por anotaciones que figuran en su base de datos e impiden la gestión de un préstamo.

RESULTANDO:

I) Que para un mejor pronunciamiento se da vista a la empresa denunciada quien presenta sus descargos, procediéndose posteriormente a dar vista de los mismos al denunciante, quien telefónicamente manifiesta su interés en que el trámite continúe.

II) Que también se procede a solicitar información adicional a la empresa denunciada, respecto a las deudas del denunciante considerando especialmente: fechas, montos y conceptos de esas deudas, reinscripciones para mantenimiento (fechas de las solicitudes), nombres de los acreedores y fechas de las cancelaciones correspondientes.

III) Que es relevante indicar que una vez recibida la información presentada por AA, se vuelve a dar vista al interesado, quien no presenta descargos.

CONSIDERANDO: I) Que se trata de una situación alcanzada por la Ley N° 18.33, de 11 de agosto de 2008 y su Decreto reglamentario N° 414/009, de 31 de agosto de 2009.

II) Que el art. 22 establece que queda expresamente autorizado el tratamiento de datos personales destinados a brindar informes objetivos, incluyendo aquéllos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticio.

III) Que dicho artículo agrega que estos datos, en el caso de personas físicas, sólo podrán estar registrados por un plazo de cinco y que en caso que al vencimiento de dicho plazo, la obligación permanezca incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. Además, las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar desde la fecha de la cancelación o extinción.

IV) Que de los descargos presentados por AA sobre todo de la información adicional aportada a instancia de la solicitud de la URCDP, surge que se ha cumplido con lo establecido en el art. 22 de la Ley.

V) Que además corresponde tener presente que el denunciante no ha presentado objeciones a la información aportada por la empresa, recomendándose así el archivo sin perjuicio, previa vista al interesado.

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

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

RESUELVE:

1- Establecer que corresponde el archivo sin perjuicio de las referidas actuaciones.

2- Notifíquese, publíquese y oportunamente archívese.

g.r.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 142/2012, de 5 de marzo de 2012.

Denuncia presentada contra dos empresas por utilizar la base de datos con la finalidad de acosar moralmente al familiar de un deudor.

| RESOLUCION No. | | Expediente No. | |
|----------------|------|----------------|---------------|
| 142 | 2012 | 2011 | 02-10-0000619 |

Montevideo, 5 de marzo de 2012.

VISTO: La denuncia formulada por AA.

RESULTANDO: I) Que AA denuncia a las empresas BB y CC manifestando que esta última ha dado un mal uso a su base de datos, con la finalidad de elaborar una estrategia de acoso moral a un familiar deudor.

II) Que se realizó el trámite correspondiente, confiriéndose vista a todas las partes involucradas, quienes las evacuaron tempestivamente.

III) Que se expidió el informe jurídico N° 15, de 9 de enero de 2012.

CONSIDERANDO: I) Que el denunciante carece de legitimación en estos autos. El tratamiento de datos en el sentido que le otorga la Ley N° 18.331 en su artículo 4º, literal M), lo fue de DD y no del denunciante.

El nombre y su asociación con la titularidad de una deuda que diera mérito al envío de una comunicación contentiva de una intimación extrajudicial de pago, se vincula a DD y no al denunciante, AA, de quien se utilizó la información proveniente de la guía telefónica (domicilio y número asociado) a los solos efectos de contactar a otra persona (artículo 9º, literal C) LPDP).

II) Que la comunicación al teléfono móvil del denunciante, número cuya obtención no resulta del todo clara, no da mérito por sí sola para imponer sanciones.

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

RESUELVE:

1. Proceder al archivo de las presentes actuaciones.
2. Notifíquese y publíquese.

m.j.r.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 172/2012, de 15 de marzo de 2012.

Se resuelve sobre Código de Conducta para el Funcionamiento de la Base Positiva y Anexo referente a Categoría de Datos a incluir en la base de datos respectiva, por parte de empresa que brinda información de carácter objetivo.

| RESOLUCION No. | | Expediente No. | |
|----------------|-----|----------------|---------|
| 172 | 011 | 2011-2-10 | 0000220 |

Montevideo, 15 de marzo de 2012.

VISTO: La presentación de AA S.A. ante la Unidad, requiriendo su opinión acerca del Código de Conducta para el Funcionamiento de la Base Positiva, y Anexo referente a Categoría de Datos a incluir en la base de datos respectiva.

RESULTANDO: I) Que estudiados los documentos sometidos a examen, se le hicieron algunas observaciones al Código de Conducta, atinentes al tiempo de conservación de los datos (art. 7°), así como la necesidad legal de practicar un tratamiento objetivo de los mismos (art. 12) y atenerse al principio de finalidad conforme ley y reglamentación respectivos (art. 16).

II) Que el peticionante ha dado respuesta a éstos y otros pedidos de aclaración que se le formularan, agregando la versión corregida del Código de Conducta, y expresando “Con relación al Anexo con la categoría de datos, se mantiene el oportunamente agregado con la precisión de que los datos del cónyuge y de empleo sólo van a ser incorporados en esta base en la medida que se cuente con el consentimiento previo del titular” (folio electrónico N° 58).

CONSIDERANDO: I) Que se consideran satisfactorias las explicaciones y ajustes aportados a los documentos originalmente presentados, en respuesta a los Informes de folios electrónicos Nros. 22 y ss., 27, 35 y 38.

II) Que en su mérito se emitirá opinión favorable acerca de los mismos, sin perjuicio del análisis que corresponda realizar al momento de solicitarse el registro de la base de datos a que aluden.

III) Que no habiendo la peticionante movilizado la acción que le acuerdan los arts. 36 inc. 2° de la Ley N° 18.331, de 11 de agosto de 2008, y 15 C) del Decreto N° 414/009, de 31 de agosto de 2009 (inscripción registral del Código de Conducta), la Unidad se circunscribirá en este momento a emitir la opinión requerida, sin perjuicio de ampliar su radio de actuación en caso de ser ello solicitado.

ATENTO: lo expuesto e informes que obran en el expediente, así como los arts. 34 A) y 36 inc. 1° 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. Expresar su opinión favorable acerca del Código de Conducta para el Funcionamiento de la Base Positiva, y Anexo referente a Categoría de Datos a incluir en la base de datos respectiva, elaborado por AA S.A., con los ajustes y recomendaciones que surgen de los Considerandos de la presente Resolución.

2. Notifíquese y estese al impulso de la administrada en cuanto a futuras acciones y proveimientos de la Unidad, tales como la inscripción registral del citado Código de Conducta y su Anexo, así como de la Base de Datos Positiva que se anuncia en la consulta formulada.

m.b.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 257/2012, de 29 de marzo de 2012.

Se resuelve sobre la regularidad jurídica de la instrucción banco centrista N° 2011/0135, pidiendo que se ordene el retiro de cierta información que figuraba en un blog accesible vía internet.

| RESOLUCION No. | | EXPEDIENTE No. | |
|----------------|----|----------------|--------------|
| 257 | 12 | 2011 | 2-10-0001043 |

Montevideo, 29 de marzo de 2012.

VISTO: La petición recibida solicitando dictamen acerca de la regularidad jurídica de la instrucción banco centralista N° 2011/01351, pidiendo que se ordene el retiro de cierta información que figuraba en un blog accesible vía Internet.

RESULTANDO: Que la referida petición mereció Informe Jurídico N° 95/2011, que obra agregado en folio electrónico N° 36 del expediente.

CONSIDERANDO: I) Que la Unidad, como todo órgano estatal, actúa con arreglo al principio de especialidad, o sea en aquellos asuntos que ingresan dentro de su competencia, enmarcada en este caso en la Ley N° 18.331 y su reglamentación (cf. Sayagués Laso, Tratado Derecho Administrativo, tomo I pág. 199, 8ª edición).

II) Que la petición formulada excede el cometido de asistencia y asesoramiento dispuesto por el art. 34 lit. A de la citada ley, pretendiendo del Órgano de Contralor actuaciones que claramente no son de su competencia.

III) Que la misma Ley, por art. 34 lit. F, comete al Órgano de Contralor emitir opiniones, pero cuando ésta sea requerida por las autoridades competentes, hipótesis que no es del caso.

IV) Que a mayor abundamiento, el planteo recibido refiere a asuntos regulados por la Ley N° 18.381 de acceso a la información pública, ámbito ajeno a las competencias de la Unidad.

ATENCIÓN: A lo expuesto, al Informe Letrado agregado, y a las normas indicadas en el cuerpo de la presente,

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

RESUELVE:

1. NO HACER LUGAR A LA PETICIÓN FORMULADA, POR FALTA DE COMPETENCIA PARA ENTENDER EN LA MISMA.

2. NOTIFÍQUESE Y PUBLÍQUESE.

m.b.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 258/2012, de 29 de marzo de 2012.

Se resuelve sobre la petición de información en relación con las bases de datos personales del Centro Integral del Personal de ANTEL (CIPA) que figuran registradas ante la URCDP.

| RESOLUCIÓN No. | | Expediente No. | |
|----------------|-----|----------------|---------------|
| 258 | 012 | 2012 | -2-10-0000230 |

Montevideo, 29 de marzo de 2012.

VISTO: La petición de información sobre las bases de datos personales de ANTEL que figuran registradas ante la Unidad.

CONSIDERANDO: El derecho de toda persona a conocer la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables.

ATENTO: A lo precedentemente expuesto, al visto favorable del Asesor Letrado y a lo dispuesto por el 34 H) 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:

Informar al peticionante que ANTEL ha registrado ante esta Unidad Reguladora y de Control, las siguientes bases de datos personales:

- “Resoluciones de Directorio” (base de datos que contiene las Resoluciones de Directorio de ANTEL), registrada con el N° B3728.
- “Correo Electrónico” (sistema de correo electrónico de ANTEL) registrada con el N° B3729.
- “Sistema de Gestión de Proveedores” (gestiona la información de los proveedores de ANTEL) registrada con el N° B2440
- “SGP” (sistema de gestión de personal) registrada con el N° B2441.
- “ACM” (datos técnicos y comerciales de los servicios celulares prestados por ANCEL) registrada con el N° B2442.
- “TELELINK” (datos de los clientes de ANTEL y ANTELDATA) con el N° B2443
- “Guía Telefónica” (datos de registro de la guía) registrada con el N° B2444.

m.b.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 285/2012, de 12 de abril de 2012.

Se resuelve sobre denuncia presentada contra dos empresas por realizar llamadas sin consentimiento a efectos de ofrecer tarjetas de crédito.

| RESOLUCION No. | | EXPEDIENTE No. |
|----------------|------|-------------------|
| 285 | 2012 | 2011-2-10-0001075 |

Montevideo, 12 de abril de 2012.

VISTO: La denuncia formulada ante la Unidad Reguladora y de Control de Datos Personales contra las empresas AA y BB, el día 26 de Diciembre de 2011.

RESULTANDO: I) La denunciante manifiesta haber recibido un llamado a su teléfono que figura en la Guía Alfabética de ANTEL y Guía clasificada (Páginas Amarillas), de la empresa de nombre comercial AA ofreciéndole una tarjeta de crédito debido a sus excelentes referencias comerciales. Al solicitar conocer la fuente de obtención de sus datos, se le comunicó que fueron obtenidos de BB.

II) Con fecha 9 de Enero de 2012, se confirió vista a BB, la que fuera evacuada en tiempo y forma.

III) Con fecha 12 de Enero de 2012, se confirió vista a AA, la que fuera evacuada en tiempo y forma.

IV) Se expidió Informe Jurídico N° 125 de 7 de Marzo de 2012.

CONSIDERANDO: I) Que la oferta que AA realiza a la denunciante, así como el informe comercial de antecedentes crediticios entregados por BB a las referidas, se realizaron conforme las disposiciones de los artículos 21 y 22 de la Ley N° 18.331.

II) Que no surge acreditado el cumplimiento del deber de informar previsto en los artículos 13 y 17 de la Ley N° 18.331. Sin embargo, encontrándose los datos de la denunciante en fuentes accesibles al público, no se verifica perjuicio que amerite solicitar sanción, causado por la comunicación de sus datos por parte de AA.

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

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

RESUELVE:

1. Recomendar a la denunciante el ejercicio del derecho de retiro o bloqueo de sus datos personales de las bases detentadas por AA y BB.
2. Recomendar a AA y BB, que tengan presente el deber de informar dispuesto en los artículos 13 y 17 de la Ley N° 18.331.
3. Notifíquese y oportunamente, publíquese.

bm.

Fdo.: Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución N° 286/2012, de 26 de mayo de 2012.

Se resuelve sobre denuncia presentada contra empresa por ofrecimiento de tarjeta de crédito sin consentimiento.

| RESOLUCION No. | | Expediente No. | |
|----------------|------|----------------|---------------|
| 286 | 2012 | 2011 | 02-10-0000342 |

Montevideo, 26 de mayo de 2012.

VISTO: La denuncia formulada contra las empresas AA y BB.

RESULTANDO: I) Que el denunciante afirma que fue contactado telefónicamente con el objetivo de ofrecerle productos en atención a su perfil crediticio, no habiendo brindando nunca su consentimiento para ello.

II) Que se realizó el trámite correspondiente, confiriéndose vista a todas las partes involucradas, expidiéndose sendos informes.

CONSIDERANDO: I) Que conforme surge de obrados, se incumplió en la especie la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, por cuanto se contravino lo previsto en el artículo 21 y lo establecido en los principios generales que regula la norma.

II) Que sin perjuicio de lo anterior y habida cuenta de la potestad discrecional que ostenta el Órgano de Control, no se impondrán sanciones, atento a que existe voluntad por parte de las denunciadas de alinearse a los parámetros de la Ley.

ATENTO: A lo expuesto y a lo previsto en las disposiciones de la Ley N° 18.331 y su Decreto reglamentario N° 414/009,

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

RESUELVE:

1. Instar a las denunciadas a alinearse a los preceptos de la Ley N° 18.331 y su Decreto reglamentario.
2. Indicar que la empresa BB deberá retirar de su base de datos, los datos personales del denunciante, tal como éste solicitó en su denuncia, al amparo de lo previsto por el artículo 21, in fine.
3. Notifíquese, publíquese y oportunamente, archívese.

m.j.r.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCD

Resolución N° 288/2012, de 12 de abril de 2012.

Se resuelve sobre denuncia presentada contra empresa por envío de correos no solicitados.

| RESOLUCION No. | | EXPEDIENTE No. | |
|----------------|----|----------------|--------------|
| 288 | 12 | 2011 | 2-10-0000977 |

Montevideo, 12 de abril de 2012.

VISTO: La denuncia presentada por envío de correos no solicitados.

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

II) Que la denunciada no compareció a tomar la vista que se le confiriera, no obstante la notificación por telegrama recibida al efecto.

CONSIDERANDO: I) Que la hipótesis denunciada encuadra como "spam", vale decir comunicación no solicitada, realizada por vía electrónica.

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

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

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

ATENTO: A lo expuesto, al Informe Letrado agregado, y a lo dispuesto por los artículos 1°, 4° D), 21, 28, 29 y 35 1) de la Ley N° 18.331, de 11 de Agosto de 2008 y su modificativa Ley N° 18.719, de 27 de diciembre de 2010,

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

RESUELVE:

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

m.b.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 289/2012, de 12 de abril de 2012.

Se resuelve sobre denuncia presentada contra empresa por tratamiento excesivo de datos personales, ya que el denunciante entiende que no corresponde se solicite copia de su cédula de identidad a los beneficiarios de sus promociones.

| RESOLUCION No. | | Expediente No. | |
|----------------|------|----------------|---------------|
| 289 | 2012 | 2011 | 02-10-0000978 |

Montevideo, 12 de abril de 2012.

VISTO: La denuncia formulada contra AA por tratamiento excesivo de datos personales.

RESULTANDO: I) Que el denunciante afirma que resulta un abuso que AA exija fotocopia de cédula de identidad a los beneficiarios de sus promociones.

II) Que se realizó el trámite correspondiente, confiriéndose vista a las partes y se expidió el informe jurídico N° 93, de 17 de febrero de 2012.

CONSIDERANDO: I) Que el artículo 7° de la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data regula el principio de veracidad estableciendo un límite en la recolección y tratamiento de los datos, a aquellos que sean veraces, adecuados, ecuanimes y no excesivos en consonancia con la finalidad para la cual se hubieren obtenido.

II) Que en el caso, la exigencia de fotocopia de cédula de identidad en las promociones otorgadas por la denunciada, indican que esta práctica resulta excesiva e inadecuada. La acreditación ante el organizador que la promoción fue efectivamente entregada al cliente se verifica con el llenado de un formulario, cuya exigencia también es requerida por el denunciado, donde constan los datos personales de nombre, cédula de identidad, número de teléfono y firma.

ATENTO: A lo expuesto y a lo previsto en las disposiciones de la Ley N° 18.331 y su Decreto reglamentario N° 414/009,

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

RESUELVE:

1. Instar a AA a que cese en la exigencia de solicitar a los beneficiarios de sus promociones, fotocopia de documento de identidad, requiriéndole únicamente su exhibición.

2. Notifíquese y publíquese.

m.j.r.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 301/2012, de 19 de abril de 2012.

Se resuelve sobre denuncia formulada contra una institución bancaria por realizar un tratamiento del teléfono celular del denunciante sin su consentimiento.

| RESOLUCION No. | | Expediente No. | |
|----------------|------|----------------|---------------|
| 301 | 2012 | 2012 | 02-10-0000070 |

Montevideo, 19 de abril de 2012.

VISTO: La denuncia formulada contra AA.

RESULTANDO: I) Que el denunciante afirma que la institución bancaria realizó un tratamiento no consentido de su dato personal, número de teléfono celular.

II) Que se dio el trámite correspondiente, oyéndose a las partes involucradas.

CONSIDERANDO: I) Que en el caso no hubo tratamiento de datos personales en el sentido que le otorga la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, en su artículo 4°, literal M), como “operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias”.

III) Las llamadas telefónicas que se verificaron al teléfono celular lo fueron a los solos efectos de contactarse con el denunciante a fin de obtener la devolución de un monto dinerario que la entidad bancaria tenía a su favor.

III) Tal extremo, justifica la mentada comunicación, pues resulta lógico, razonable y legítimo el uso de un mecanismo directo que permita la localización de un cliente a esos efectos.

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

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

RESUELVE:

1. Proceder al archivo de las presentes actuaciones.
2. Notifíquese y publíquese.

m.j.r.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 654/2012, de 5 de julio de 2012.

Se resuelve sobre denuncia presentada contra empresa pública debido a que se atribuye a la denunciante un contrato que ya ha sido otorgado a otra persona de igual nombre.

| RESOLUCION N° | | EXPEDIENTE N° |
|---------------|------|-------------------|
| 654 | 2012 | 2012-2-10-0000254 |

Montevideo, 05 de julio de 2012.

VISTO: La denuncia presentada contra AA y BB debido a que por error de tipeo de un funcionario de AA, se le atribuye a la denunciante un contrato que ha sido otorgado a favor de otra persona que se llama igual y vive en Maldonado.

RESULTANDO: I) Que de acuerdo con la denuncia la interesada sólo fue informada al presentar su reclamo, por lo cual además solicita acceder a la siguiente información: si está en el sistema y si está por qué razón, así como obtener copia del contrato, el registro de su reclamo y constancia de la solución del problema.

II) Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista a ambos organismos, realizándose posteriormente el informe jurídico correspondiente.

III) Que AA afirma que una vez recibido el reclamo se constató que efectivamente al poseer en la base los datos de varias personas que tienen el mismo nombre y apellido, por error, se cargó el contrato a nombre de la denunciante, pero que inmediatamente se procedió a subsanar tal error.

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

II) Que respecto al error, cabe concluir que según los argumentos presentados por AA, -y que la denunciante no ha controvertido-, una vez recibido el reclamo y constatado el mismo, se ha procedido a subsanar el mismo en forma inmediata, de acuerdo a lo previsto en el art. 15 de la Ley.

III) Que en cuanto al derecho de acceso, el art. 14 de la Ley establece que todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas.

IV) Que en este sentido, corresponde solicitar a este organismo que proporcione en determinado plazo, toda la información que posee sobre la denunciante en sus bases de datos, incluyendo todo lo relacionado con este incidente, el trámite de su reclamo y la solución adoptada, salvaguardando los datos personales de los terceros ajenos al mismo.

ATENCIÓN: A lo expuesto y a lo previsto en las normas legales citadas,
LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES
RESUELVE:

1. Otorgar a AA un plazo de 10 días a efectos de que garantice a la denunciante el derecho consagrado en el art. 14 de la Ley.
2. Notifíquese, publíquese y oportunamente archívese.

g.r.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 674/2012, de 19 de julio de 2012.

Se impugna Resolución N° 1658/2011 recaída en el expediente sobre publicación en la web de información sobre sanciones de profesionales por parte de organismo encargado de la superintendencia y control.

| RESOLUCION No. | | Expediente No |
|----------------|------|-------------------|
| 674 | 2012 | 2011-2-10-0000079 |

Montevideo, 19 de julio de 2012.

VISTO: Estos obrados en los cuales se impugna la Resolución N° 1658/2011 recaída en el expediente.

CONSIDERANDO: I) Que posteriormente a la instrucción del recurso de revocación y la emisión del informe jurídico N° 114/2012, la impugnante fundamentó los agravios oportunamente expresados, según la reserva realizada.

II) Que en el numeral 4) de su escrito de fundamentación, señala la postura abierta y flexible del organismo de control para realizar ajustes y perfeccionar el sistema actualmente utilizado, que motivara la denuncia considerada en el presente caso.

III) Que existen alternativas mediante las cuales el responsable de un sitio web puede restringir o impedir que cierta información sea indexada por los motores de búsqueda, según surge del informe a fs. 90, cuyas aplicaciones para la Administración Central serán objeto de instrucción por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic).

IV) Que reexaminada la situación fáctica a la luz de los fundamentos expuestos, se entiende que corresponde revisar el criterio adoptado en la especie, sin perjuicio de lo expuesto en el anterior "Considerando" a fin de la protección de la situación jurídica del denunciante.

ATENTO: A lo precedentemente expuesto,

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

RESUELVE:

1. Dejar sin efecto la Resolución N° 1658/2011 de 7 de diciembre de 2012.
2. Recomendar al organismo, en su calidad de responsable de un sitio web, la pertinencia de utilizar alternativas técnicas que le permitan restringir o impedir que cierta información sea indexada por los motores de búsqueda, considerando a sus efectos las indicaciones que oportunamente realizará la Agesic.
3. Notifíquese personalmente a las partes, comuníquese a la Presidencia de la República y oportunamente archívese.

b.m.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Resolución N° 699/2012, de 9 de agosto de 2012.

Se resuelve sobre informe del artículo 291 del Proyecto de Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al Ejercicio 2011, que refiere a la posibilidad de mantener los datos inscriptos en la Central de Riesgos, una vez vencidos los plazos correspondientes.

| RESOLUCIÓN No. | | ACTA No. | |
|----------------|------|----------|----|
| 699 | 2012 | 2012 | 29 |

Montevideo, 9 de Agosto de 2012.

VISTO: el art. 291 del proyecto de Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al Ejercicio 2011.

RESULTANDO: Que se proyecta incorporar al artículo 2° de la Ley 18.812, de 23 de setiembre de 2011, el siguiente inciso a continuación del primero: "Sin perjuicio de lo dispuesto en el inciso precedente, una vez transcurrido el plazo para que los datos permanezcan inscriptos en la Central de Riesgos Crediticios, el Banco Central del Uruguay podrá mantenerlos como datos estadísticos con el único fin de realizar estudios de riesgo de crédito para el desarrollo de sus funciones de regulación, adquiriendo tales datos, en este caso, carácter confidencial."

CONSIDERANDO: I) Que la Ley de Protección de Datos y Acción de Habeas Data, N° 18.331, de 11-VIII-2008, art. 8°, prevé que los datos objeto de tratamiento "deben ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubieren sido recolectados", sin perjuicio de referir a "casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya perimido tal necesidad o pertinencia".

II) Que los fines estadísticos que fundamentan el texto proyectado pueden adecuarse a la normativa de protección de datos más allá del plazo que prevé la Ley N° 18.812, disponiéndose al efecto un procedimiento de disociación de la información que conserve el Banco Central, de acuerdo con lo previsto por el art. 17 apartado "D" de la Ley 18.331.

III) Que, para el caso de no disociarse de modo que los titulares de datos no sean identificables, resulta pertinente establecer el carácter secreto de la información de referencia, acorde con el criterio general del sistema estadístico nacional y, por otra parte, en el marco de lo estatuido por la Ley N° 18.381, de 17-X-2008, art. 8°.

ATENTO: a lo expuesto,

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

RESUELVE:

1. Hacer saber a la Presidencia de la República las circunstancias y consideraciones que figuran en este acto, acompañándose copia del mismo.

2. Formular los siguientes textos alternativos de la norma citada en el “Visto” de la presente:
A) “Artículo 291. “Incorpórase al artículo 2° de la Ley N° 18.812, de 23 de setiembre de 2011 el siguiente inciso a continuación del primero:

“Sin perjuicio de lo dispuesto en el inciso precedente, una vez transcurrido el plazo para que los datos permanezcan inscriptos en la Central de Riesgos, el Banco Central del Uruguay podrá mantenerlos disociados como datos estadísticos con el único fin de realizar estudios de riesgo de crédito para el desarrollo de sus funciones de regulación”.

B) Artículo 291. “Incorpórase al artículo 2° de la Ley N° 18.812, de 23 de setiembre de 2011 el siguiente inciso a continuación del primero:

“Sin perjuicio de lo dispuesto en el inciso precedente, una vez transcurrido el plazo para que los datos permanezcan inscriptos en la Central de Riesgos, el Banco Central del Uruguay podrá mantenerlos como datos estadísticos con el único fin de realizar estudios de riesgo de crédito para el desarrollo de sus funciones de regulación, adquiriendo tales, en este caso, carácter de secretos”.

g.r.

Fdo.: Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 700/2012, de 9 de agosto de 2012.

Se resuelve sobre informe relativo al artículo 264 del Proyecto de Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al Ejercicio 2011, que refiere a la ampliación de las facultades otorgadas a la Dirección General Impositiva (DGI) ante las cuales no regirán las limitaciones establecidas en la Ley N° 18.331.

| RESOLUCIÓN No. | | ACTA No. | |
|----------------|------|----------|----|
| 700 | 2012 | 2012 | 29 |

Montevideo, 9 de Agosto de 2012.

VISTO: el art. 264 del proyecto de Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al Ejercicio 2011.

RESULTANDO: Que la citada disposición proyectada, en sus dos primeros incisos, expresa: “Las facultades establecidas por el artículo 68 del Código Tributario autorizan a la Dirección General Impositiva a solicitar información tanto en el marco de una actuación inspectiva particular como con carácter general mediante resolución fundada del organismo recaudador. A los efectos de lo establecido en el presente artículo, no regirán las limitaciones dispuestas en la Ley No. 18.331, de 11 de agosto de 2008”.

CONSIDERANDO: I) Que las facultades que se asignan por ley a un órgano estatal para desarrollar sus respectivos cometidos deben insertarse en el régimen jurídico de la Protección de Datos Personales, la cual está comprendida como derecho fundamental, inherente a la personalidad humana (arts. 72 de la Constitución y 1° de la citada ley).

II) Que, por lo mismo, los objetivos que fundamentan la norma proyectada no pueden determinar que se deje de lado las “limitaciones dispuestas” en esa ley, de manera general y absoluta. Ello implicaría, en efecto, la afectación de derechos de las personas a asegurar que los datos que se recojan a los fines de su tratamiento sean veraces y adecuados; a que no se utilicen para fines distintos o incompatibles con los que motivaron su obtención; a que quien los posee –en el caso sería la Administración Tributaria – adopte las medidas de seguridad necesarias para evitar su pérdida o tratamiento no autorizado; a que el titular de los datos pueda solicitar la rectificación o actualización, etc.

III) Que los referidos objetivos pueden contemplarse con soluciones legales que faciliten la cesión de datos a la Administración Tributaria, la cual está regulada de modo general por el art. 17 de la Ley N° 18.331, tal como se ha hecho en Derecho comparado (ejemplo art. 94 de la Ley General Tributaria de España, N° 58 de 17-XII-2003).

ATENCIÓN: a lo expuesto,

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

RESUELVE:

1.Hacer saber a la Presidencia de la República las circunstancias y consideraciones que figuran en este acto, acompañándose copia del mismo.

2.Propiciar el siguiente texto alternativo de la norma citada en el “Visto” de la presente:

“ARTÍCULO 264.- Las facultades establecidas por el artículo 68 del Código Tributario autorizan a la Dirección General Impositiva a solicitar información tanto en el marco de una actuación inspectiva particular como con carácter general mediante resolución fundada del organismo recaudador, la cual contemplará lo pertinente en materia de protección de datos personales.

A los efectos de lo establecido en esta disposición, no será necesario el previo consentimiento de los interesados, en aplicación de los arts. 9º inciso 3º literal B), y 17 de la Ley N° 18.331, de 11 de agosto de 2008.

Quien incumpliera la obligación de proporcionar la información en el ámbito del presente artículo, será sancionado con multa de hasta mil veces el valor máximo de la multa por contravención (artículo 95 del Código Tributario) de acuerdo a la gravedad del incumplimiento (artículo 100 del Código Tributario)”.

m.b.

Fdo.: Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 810/2012, de 6 de setiembre de 2012.

Se resuelve sobre denuncia presentada contra empresa por incluir en la guía telefónica, nombre y teléfono del denunciante sin su consentimiento.

| RESOLUCION No. | | EXPEDIENTE No. |
|----------------|------|-------------------|
| 810 | 2012 | 2011-2-10-0000418 |

Montevideo, 6 de setiembre de 2012.

VISTO: La denuncia presentada ante esta unidad contra AA por incluir en la guía el nombre y teléfono del denunciante sin su consentimiento.

RESULTANDO: I) Que con fecha 8 de noviembre de 2011 presenta la denunciada la impresión de un correo electrónico donde aparece el denunciante como confirmado con fecha 24 de setiembre de 2010, pero no se indica que consiente el tratamiento de sus datos

II) Que con fecha 17 de noviembre del corriente, la empresa denunciada tomó vista del informe jurídico N° 6972, que solicitaba la presentación de los formularios de inscripción de bases de datos personales de AA.

CONSIDERANDO: I) Que de acuerdo a lo establecido en el artículo 9° de la Ley N° 18.331 para que los datos puedan ser tratados, se requiere el consentimiento previo del titular. En este caso se presenta un correo electrónico donde figuran los datos del denunciado, lo que no prueba que efectivamente se haya consentido el tratamiento.

II) Que por el artículo 35 de la citada Ley, la URCDP cuenta con potestades sancionatorias, las cuales puede ejercer en caso de contravención a la normativa vigente en materia de protección de datos personales.

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

RESUELVE:

1. RECOMENDAR AL DENUNCIANTE QUE EJERZA SU DERECHO DE SUPRESIÓN EN LOS TÉRMINOS DEL ARTÍCULO 15 DE LA LEY N° 18.331.
2. SANCIONAR CON OBSERVACIÓN AAA POR CONTRAVENCIÓN AL ARTÍCULO 9° DE LA LEY N° 18.331.
3. ESTABLECER QUE AA, DEBERÁ PRESENTAR LOS FORMULARIOS PARA REALIZAR LA INSCRIPCIÓN DE LAS BASES DE DATOS PERSONALES, DENTRO DEL PLAZO DE 30 DÍAS.
4. NOTIFÍQUESE Y PUBLÍQUISE.

r.i.

Fdo.: Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 811/2012, de 6 de setiembre de 2012.

Se resuelve sobre denuncia presentada contra institución bancaria por el envío de una tarjeta de crédito promocional, expedida por una compañía de telefonía de la cual el denunciante no es cliente.

| RESOLUCION No. | | EXPEDIENTE No. |
|----------------|------|-------------------|
| 811 | 2012 | 2011-2-10-0000813 |

Montevideo, 6 de setiembre de 2012.

VISTO: La denuncia presentada ante esta unidad contra entidad bancaria AA, por el envío de una tarjeta de crédito promocional expedida por dicha entidad y una compañía de telefonía de la cual el denunciante no es cliente.

RESULTANDO: I) Que con fecha 15 de diciembre de 2011 se presenta AA, donde indica que el error ya fue solucionado y la modificación de los datos comunicada al denunciante, presentando la constancia correspondiente.

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

CONSIDERANDO: I) Que de acuerdo a lo establecido en el artículo 15 de la Ley N° 18.331 toda persona tiene derecho a solicitar que se rectifiquen sus datos incluidos en una base de datos, que sean incorrectos. Como contrapartida, el responsable de la base de datos debe rectificar el dato incorrecto y notificar al titular.

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

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

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

RESUELVE:

1. RECOMENDAR AL DENUNCIANTE QUE EJERZA SU DERECHO DE ACCESO EN LOS TÉRMINOS DEL ARTÍCULO 14 DE LA LEY N° 18.331, A FIN DE CONSTATAR SI SUS DATOS FUERON ELIMINADOS.
2. RECOMENDAR A LA ENTIDAD BANCARIA AA RECABAR EL CONSENTIMIENTO DE SUS USUARIOS, EN LOS TÉRMINOS DEL ARTÍCULO 9° DE LA LEY N° 18.331.
3. NOTIFÍQUESE Y PUBLÍQUISE.

r.i.

Fdo.: Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 871/2012, de 20 de setiembre de 2012.

Se resuelve sobre denuncia presentada contra empresa por el envío de correos electrónicos sin consentimiento.

| RESOLUCION N° | | EXPEDIENTE N° |
|---------------|------|-------------------|
| 871 | 2012 | 2011-2-10-0000586 |

Montevideo, 20 de setiembre de 2012.

VISTO: La denuncia formulada ante la Unidad Reguladora y de Control de Datos personales por AA contra la empresa BB por envío de correos electrónicos sin su consentimiento.

RESULTANDO: I) Que AA manifiesta que ha recibido correos electrónicos no deseados procedentes de la casilla de correo xxx@adinet.com.uy, correspondiente a la empresa BB y que desconoce cómo han accedido a éste. Alega haber solicitado a través de correos electrónicos ser removido de la lista, no obteniendo respuestas. Como prueba de sus dichos, agrega correos electrónicos recibidos.

II) Que la empresa BB evacuó tempestivamente la vista conferida indicando que la suscripción a la red es voluntaria y puede ser realizada por el interesado o cualquier persona. En cuanto a las solicitudes de baja de la lista de suscriptores, alega que la casilla del correo a la cual fueron enviadas no cuenta con la posibilidad de enviar respuesta. De los descargos formulados por la empresa no resulta probado que el denunciante hubiese consentido el tratamiento de su correo electrónico a fin de recibir ofertas de empleo.

CONSIDERANDO: I) Que resulta acreditado el envío por parte de la empresa denunciada de correos electrónicos no deseados (Spam) a la casilla de correo del denunciante.

II) Que no resultó probado que el denunciante hubiese consentido el tratamiento de su correo electrónico a fin de recibir ofertas de empleo, no contando la empresa denunciada con las medidas necesarias para cumplir con las disposiciones legales en materia de consentimiento previstas en la Ley N° 18.331. En ese sentido se entiende que el consentimiento no fue prestado.

III) Que corresponde tener en cuenta la primariedad de la infracción cometida.

ATENTO: Al Informe glosado y en función de lo preceptuado en los artículos 9 y 35 de la Ley N° 18.331, este último en su redacción dada por el artículo 152 de la Ley N° 18.719, de 27 de Diciembre de 2010.

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

1. SANCIONAR CON “OBSERVACIÓN” A BB POR INFRACCIÓN A LA LEY N° 18.331 AL TRATAR EL DATO PERSONAL CORREO ELECTRÓNICO SIN CONSENTIMIENTO DE SU TITULAR Y ENVIAR COMUNICACIONES ELECTRÓNICAS NO SOLICITADAS.
2. ESTABLECER QUE LA EMPRESA DEBERÁ ADOPTAR LAS MEDIDAS NECESARIAS PARA ADECUAR EL SISTEMA DE SUSCRIPCIÓN Y DADA DE BAJA DE SU RED A LAS DISPOSICIONES DE LA LEY N° 18.331.
3. NOTIFÍQUESE Y PUBLÍQUESE.

j.h.

Fdo.: Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Resolución N° 931/2012, de 18 de octubre de 2012.

Se resuelve denuncia contra periódico barrial por incluir datos personales de los funcionarios de un complejo de viviendas.

| RESOLUCION N° | | EXPEDIENTE N° |
|---------------|------|-------------------|
| 931 | 2012 | 2012-2-10-0000451 |

Montevideo, 18 de octubre de 2012.

VISTO: La denuncia presentada contra el editor del periódico "ZZ", por entender que éste ha vulnerado la Ley de Protección de Datos, al utilizar sin el consentimiento los nombres e información relacionada con funcionarios del complejo (sueldos y demás información que se intercambia en las asambleas), en este medio de difusión.

RESULTANDO: I) Que de acuerdo con la denuncia, si bien el denunciado es Presidente de uno de los bloques del complejo, el periódico es un emprendimiento privado de carácter personal, por esa razón ellos no autorizan que sus datos personales sean utilizados; utilización que además le ha generando una opinión que los perjudica, hiere su integridad y su sensibilidad.

II) Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista a ambas partes, y se han presentado los descargos correspondientes.

III) Que el denunciado agrega copia de las publicaciones emitidas luego de recibida la nota de los denunciantes (15 de junio de 2011) y en las mismas ya no se identifican datos personales que causen un perjuicio a los denunciantes o vulneren la Ley N° 18.331.

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

II) Que sin embargo, la utilización de los nombres y demás información relacionada, debe ser analizada en el contexto en el cual se desarrolla y ponderando los demás derechos que entran en juego, pues se trata de una publicación o medio de prensa que ha sido inscripta en el registro del MEC, por ello deben ser sopesados los demás derechos y libertades relacionadas con la posibilidad de comunicar e informar.

III) Que en este sentido, leída la información contenida en varios de los periódicos emitidos luego del 15 de julio de 2011, no se identifica información de carácter personal que no debería ser publicada porque vulnera la integridad y sensibilidad de los denunciantes, tampoco surgen datos que podrían considerarse excesivos o desproporcionados de acuerdo con la finalidad que poseen las publicaciones.

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

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Establecer que se ha producido una corrección de la información personal que contiene el periódico, la cual debe ser mantenida a los efectos del cumplimiento de la Ley N° 18.331.
2. Indicar que no obstante ello, corresponde la inscripción de las bases de datos que se posean tanto a nivel del medio de prensa como del complejo de viviendas.
3. Notifíquese, publíquese y oportunamente archívese.

g.r.

Fdo.: Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Resolución N° 982/2012, de 15 de noviembre de 2012.

Se resuelve denuncia en la cual se alega no haber logrado en tiempo y forma la eliminación de sus datos personales en una base de datos utilizada para promoción de servicios de parte de la institución bancaria denunciada.

| RESOLUCION No. | | Expediente No. | |
|----------------|-----|----------------|--------------|
| 982 | 012 | 2011 | 2-10-0001086 |

Montevideo, 15 de noviembre de 2012.

VISTO: La denuncia recibida por persona física que alega no haber logrado en tiempo y forma la eliminación de sus datos personales en una base de datos utilizada para promoción de servicios de parte de la institución bancaria denunciada.

RESULTANDO: I) Que la denunciante acompaña prueba emergente de sucesivos correos electrónicos intercambiados con la denunciada, de la que surge que a lo largo de un año rechazó la tarjeta de crédito ofrecida y solicitó que no se le enviaran más los estados de cuenta con cargo a emisión de la misma.

II) Que la denunciada expresó en su descargo ante la Unidad que las disposiciones banconcentralistas le obligan a mantener el registro de datos de sus clientes, al tiempo de reconocer que hubo demoras en proceder al bloqueo de dichos datos por circunstancias de índole técnica, no así por intencionalidad ni despreocupación en hacerlo.

CONSIDERANDO: I) Que la Ley N° 18.331 es clara en cuanto al derecho del titular del dato de solicitar el retiro o bloqueo de sus datos en aquellas bases con fines de publicidad (art. 21) prescribiendo un plazo de cinco días hábiles para cumplir con dicha solicitud (art. 15).

II) Que la denunciante no recibió la atención debida a su solicitud de baja del tratamiento de sus datos personales a fines publicitarios, prologándose el tratamiento indebido por más de un año.

III) Que los descargos expresados para justificar esta falta de servicio son genéricos e insuficientes.

IV) Que la Unidad aplicó sanción a la denunciada con anterioridad (Exp. N° 674/2011), recurrida en vía administrativa actualmente en trámite.

ATENTO: A lo expuesto; al Informe Letrado; a los arts. 15, 21 y 35 de la Ley N° 18.331, de 11 de Agosto de 2008; y a la Resolución N° 320, de 17 de Marzo de 2011,

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

RESUELVE:

1. SANCIONAR CON MULTA DE 1.500 (MIL QUINIENTAS) UNIDADES INDEXADAS A BANCO AA POR INFRACCIÓN A LA LEY N° 18.331 (NO ATENDER EN TIEMPO Y FORMA UNA SOLICITUD DE BLOQUEO DE DATOS PERSONALES).

2. NOTIFÍQUESE Y PUBLÍQUESE.

m.b.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 1034/2012, de 13 de diciembre de 2012.

Se resuelve sobre denuncia presentada contra institución pública educativa por el uso de imágenes tomadas por las cámaras de videovigilancia como prueba en un procedimiento sumarial.

| RESOLUCION No. | | EXPEDIENTE No. |
|----------------|------|-------------------|
| 1034 | 2012 | 2012-2-10-0000558 |

Montevideo, 13 de diciembre de 2012.

VISTO: La denuncia presentada ante esta Unidad contra la entidad educativa AA de la Universidad de la República por el uso de imágenes tomadas de cámaras de videovigilancia como prueba en un procedimiento sumarial.

RESULTANDO: I) Que con fecha 6 de julio de 2012 se realiza un acta de constatación de los DVD agregados como prueba por parte del denunciante, de dicha acta surge que se verifica la presencia del mismo.

II) Que con fecha 12 de octubre del corriente, la denunciada tomó vista del informe jurídico N° 454, que solicitaba la presentación de los formularios de inscripción de bases de datos de videovigilancia.

CONSIDERANDO: I) Que la URCDP se pronunció en el Dictamen N° 10 de 16 de abril de 2010, respecto a la videovigilancia, en el sentido que resulta de aplicación la normativa vigente en materia de datos personales.

II) Que como existe registro de las imágenes constituye una base de datos personales, atento a que puede existir tratamiento de datos y de la misma manera, el titular de dichos datos puede ejercer los derechos de acceso, inclusión, supresión y modificación establecidos en la Ley N° 18.331.

ATENTO: A lo precedentemente expuesto y a lo dispuesto por le Ley N° 18.331.

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

RESUELVE:

1. ESTABLECER QUE EXISTIÓ POR PARTE DE LA DENUNCIADA UNA CONTRAVENCIÓN AL PRINCIPIO DE LEGALIDAD ESTABLECIDO EN EL ARTÍCULO 6° DE LA LEY N° 18.331.
2. INDICAR QUE LA DENUNCIADA DEBERÁ PRESENTAR LOS FORMULARIOS PARA REALIZAR LA INSCRIPCIÓN DE LA BASE DE DATOS DE VIDEOVIGILANCIA, DENTRO DEL PLAZO DE 30 DÍAS.
3. NOTIFÍQUESE Y PUBLÍQUISE.

r.i.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 1035/2012, de 13 de diciembre de 2012.

Se resuelve sobre denuncia presentada contra institución pública educativa por la existencia de bases de datos que no se encuentran inscriptas.

| RESOLUCION No. | | EXPEDIENTE No. |
|----------------|------|-------------------|
| 1035 | 2012 | 2012-2-10-0000559 |

Montevideo, 13 de diciembre de 2012.

VISTO: La denuncia presentada ante esta unidad contra la entidad educativa AA de la Universidad de la República por la existencia de bases de datos que no se encuentran inscriptas.

RESULTANDO: I) Que con fecha 16 de julio de 2012 la denunciada manifiesta que sus bases de datos se encuentran centralizadas en BB. Adjuntan como prueba una nota fechada el 11 de julio donde la Unidad de Informática manifestando que las bases de datos están en “trámite de registro”.

II) Que con fecha 11 y 12 de octubre respectivamente, BB y AA toman vista del informe jurídico N° 475, que solicita la presentación los formularios de inscripción de las bases de datos personales.

CONSIDERANDO: I) Que la URCDP se pronunció en la Resolución N° 1288 de 3 de setiembre de 2010, apercibiendo a la Universidad de la República para que inscriba sus bases de datos personales.

II) Que existe por parte de los responsables de bases de datos personales la obligación de respetar los principios de la protección de datos tales como el principio de legalidad, que implica inscribir las bases de datos personales. Asimismo debe informar a los titulares de los datos acerca de cómo ejercer los derechos de acceso, inclusión, supresión y modificación establecidos en la Ley N° 18.331.

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

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

RESUELVE:

1. ESTABLECER QUE EXISTIÓ POR PARTE DE AA Y DE BB UNA CONTRAVENCIÓN AL PRINCIPIO DE LEGALIDAD ESTABLECIDO EN EL ARTÍCULO 6° DE LA LEY N° 18.331.
2. INDICAR QUE BB DEBERÁ PRESENTAR LOS FORMULARIOS PARA REALIZAR LA INSCRIPCIÓN DE LAS BASES DE DATOS PERSONALES, DENTRO DEL PLAZO DE 30 DÍAS.
3. NOTIFÍQUESE Y PUBLÍQUESE.

r.i.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 1036/2012, de 13 de diciembre de 2012.

Se resuelve sobre denuncia presentada contra una institución bancaria por el envío de tarjeta de crédito sin consentimiento.

| RESOLUCION No. | | EXPEDIENTE No. |
|----------------|------|-------------------|
| 1036 | 2012 | 2011-2-10-0000697 |

Montevideo, 13 de diciembre de 2012.

VISTO: La denuncia presentada ante esta unidad contra entidad bancaria AA, por el envío de una tarjeta de crédito promocional no solicitada.

RESULTANDO: I) Que en tiempo y forma se presenta el Banco denunciado donde indica que los datos del titular ya fueron eliminados de la base de datos.

II) Que los datos del denunciante fueron aportados como una referencia personal, de un cliente del Banco.

CONSIDERANDO: I) Que de acuerdo a lo establecido en el artículo 15 de la Ley N° 18.331 toda persona tiene derecho a solicitar que se rectifiquen sus datos incluidos en una base de datos, que sean incorrectos. Como contrapartida, el responsable de la base de datos debe rectificar el dato incorrecto y notificar al titular.

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

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

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

1. HACER SABER AL DENUNCIADO QUE EXISTIÓ UNA CONTRAVENCIÓN AL PRINCIPIO DE FINALIDAD CONSAGRADO EN EL ARTÍCULO 8° DE LA LEY N° 18.331, CONDUCTA QUE NO DEBERÁ REPETIRSE.

2. RECOMENDAR AL DENUNCIANTE QUE EJERZA SU DERECHO DE ACCESO EN LOS TÉRMINOS DEL ARTÍCULO DE LA CITADA LEY, A FIN DE CONSTATAR SI SUS DATOS FUERON ELIMINADOS.

III. NOTIFÍQUESE Y PUBLÍQUISE.

r.i.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 1040/2012, del 20 de diciembre de 2012.

Se resuelve sobre informe técnico brindado por el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), respecto a las posibilidades que brinda la tecnología para evitar que ciertos contenidos sean indexados e incluidos en el caché de los buscadores de internet, a efectos de garantizar la protección de datos personales y en especial el derecho al olvido.

| RESOLUCIÓN N° | | EXPEDIENTE N° |
|---------------|------|-------------------|
| 1040 | 2012 | 2012-2-10-0000634 |

Montevideo, 20 de diciembre de 2012.

VISTO: La solicitud de informe técnico al CERT-uy, sobre posibles soluciones técnicas para evitar que ciertos contenidos sean indexados e incluidos en el caché de los buscadores de Internet, con posible afectación del derecho a la Protección de Datos Personales.

RESULTANDO: I) Que toda persona física o jurídica, que publica determinado contenido, tiene que colaborar con su posterior eliminación si ello es solicitado, pues no es posible eliminar un contenido particular de Internet sin la intervención de quien lo publicó.

II) Que se trata de determinar si desde el punto de vista técnico, es posible evitar que ciertos contenidos, que fueron borrados de Internet, permanezcan indexados y sean mostrados por los buscadores de páginas web.

CONSIDERANDO: I) Que los buscadores periódicamente recorren las páginas web, creando una base de datos y un "caché" con lo que buscan en ellas, de modo de facilitar las próximas búsquedas e indexando además los contenidos (crawling). Esto hace que incluso una vez modificado el sitio real, exista una "copia" del contenido en los sitios de los buscadores.

II) Que cada buscador tiene su propia política de "caché", por ello en algunos casos es posible advertir que no se desea incluir en el "caché" determinado contenido, mientras que en otros casos hay que solicitar que se elimine posteriormente.

III) Que en todo caso procede la adopción de medidas preventivas a saber:

a) que los documentos se generen en tiempo real en lugar de que sean generados previamente, de forma que no se puedan almacenar porque simplemente no existen en el momento en que se buscan, controlando así su propagación.

b) que la publicación de información con datos personales se efectúe en formato imagen con etiquetas o atributos que no contengan esos datos.

ATENTO: a lo precedentemente expuesto,

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

RESUELVE:

1. Recomendar a los responsables de publicar contenidos en los sitios web de los organismos públicos, la adopción de alguno de los criterios técnicos señalados en la parte expositiva de este acto, que se desarrollan en el informe técnico del CERT-uy, que se incorpora a esta Resolución.

2. Comuníquese, publíquese y oportunamente, archívese.

g.r.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 1041/2012, de 20 de diciembre de 2012.

Se resuelve sobre inscripción de Código de Conducta.

| RESOLUCION No. | | Expediente No. | |
|----------------|-----|----------------|---------|
| 1041 | 012 | 2012-2-10 | 0000466 |

Montevideo, 20 de diciembre de 2012.

VISTO: La comparecencia de AA S.A. ante la Unidad, solicitando la inscripción del Código de Conducta denominado "Pautas para la Conducta en los Negocios" cuyo texto acompaña.

RESULTANDO: I) Que se trata de un texto proveniente del Grupo Empresarial Internacional al que pertenece la compareciente, que contiene el conjunto de normas de conducta que deben observar los directivos y empleados del grupo.

II) Que en su parte central contiene seis principios de actuación, dos de los cuales presentan relación con la materia sujeta a control de esta Unidad.

CONSIDERANDO: I) Que el Código de Conducta cuya aprobación se solicita resulta correcto en tanto código de conducta general, no obstante lo cual merece adecuarse a los criterios y detalles de un código de conducta sobre protección de datos personales.

II) Que de conformidad con la preceptiva legal, y remitiendo por extensión a lo consignado en el Informe Letrado N° 542/2012, para proceder a su aprobación será necesario que el texto a aprobar contenga ciertas previsiones, si bien mínimas, mayores que las exhibidas.

ATENCIÓN: A lo expuesto en los informes letrados que obran en el expediente, así como los art. 36 de la Ley N° 18.331, de 11 de agosto de 2008.

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

DICTAMINA:

1. Que el documento denominado "Pautas para la Conducta en los Negocios" puesto en consideración de la Unidad, merece opinión favorable como Código de Conducta general.
2. Que sin perjuicio de ello, y a los efectos de completar la adecuación del citado documento a un Código de Conducta relativo a Políticas de Privacidad y Protección de Datos Personales dentro de la organización, el mismo deberá adicionar los siguientes contenidos mínimos:
 - A) - "Disposiciones generales" relativas al objeto del código, ámbito de aplicación y definiciones de términos.
 - B) "Aplicación de los principios generales" del régimen general de la protección de datos en la gestión cotidiana de la organización.
 - C) "Gestión y tratamiento de las bases de datos personales" en la organización.
 - D) "Derechos de los titulares de los datos" oportunidades y formas de ejercicio.
3. Que a los efectos antes indicados la interesada tendrá que presentar un único texto a título de Código de Conducta, adecuándolo a las pautas expresadas.

m.b.

Fdo.: Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución N° 1043/2012, de 20 de diciembre de 2012.

Se resuelve adherir a la propuesta realizada por la Secretaría Permanente de la Red Iberoamericana de Protección de Datos, respecto a brindar impulso al Proyecto de Cooperación para el intercambio de información en materia de protección de datos de menores, que permita conocer los recursos disponibles y servicios tecnológicos existentes para enfrentar los riesgos que implica la utilización de las TIC y en especial Internet.

| RESOLUCION N° | | ACTA N° |
|---------------|------|---------|
| 1043 | 2012 | 48 |

Montevideo, 20 de Diciembre de 2012.

VISTO: La comunicación recibida por la Secretaría Permanente de la Red Iberoamericana de Protección de Datos.

ATENTO: A que se efectúa un planteo relativo el impulso de un Proyecto de cooperación para el intercambio de información en materia de protección de datos de menores que permita conocer los recursos disponibles y las posibilidades de compartirlos, y los servicios tecnológicos desarrollados para hacer frente a los riesgos de las TIC para la privacidad de los menores, especialmente en el ámbito de Internet.

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

RESUELVE:

ADHERIR A LA ACTIVIDAD PROPUESTA POR LA SECRETARÍA PERMANENTE DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS A LOS EFECTOS DE INTERCAMBIAR EXPERIENCIAS CON OTRAS AUTORIDADES DE PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD.

Fdo.: Dr. Felipe Rotondo

Consejo Ejecutivo URCDP



Dictámenes



Dictamen N° 1, de 15 de marzo de 2012.

Se dictamina sobre si resulta procedente la aplicación de la Ley N° 18.331 a los objetivos del grupo llamado “Apostasía Colectiva en Uruguay”

| DICTAMEN No. | | Expediente No. |
|--------------|------|--------------------|
| 1 | 2012 | 2011-2-10-00001074 |

Montevideo, 15 de marzo de 2012.

VISTO: La consulta planteada por AA solicitando asesoramiento a la Unidad Reguladora y de Control de Datos Personales.

RESULTANDO: I) AA indica haber conformado un grupo llamado “BB”, siendo de interés de ese colectivo se le informe acerca de si resulta procedente en el caso, la aplicación de las disposiciones de la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data.

II) Se expidió el informe jurídico N° 5, de 3 de enero de 2012.

CONSIDERANDO: I) Apostatar, según el diccionario de la Real Academia Española significa: “Negar la fe de Jesucristo recibida en el bautismo; Dicho de un religioso: Abandonar irregularmente la orden o instituto a que pertenece; Dicho de un clérigo: Prescindir habitualmente de su condición de tal, por incumplimiento de las obligaciones propias de su estado”.

II) En el bautismo se asienta el acto de celebración de uno de los sacramentos que otorga la Iglesia Católica, no constituyendo, por ende, un dato que pueda tildarse de inexacto total o parcialmente, erróneo o falso, para apostatar, o, como exige la normativa de protección de datos, para proceder a su rectificación, actualización o eliminación. (artículos 10, 11 y 13 del Decreto N° 414/009 y artículo 15 de la LPDP).

III) A lo anterior se añade que los datos contenidos en los libros de bautismo no configuran en sentido estricto, la categoría de bases de datos, sino simplemente un conglomerado de datos que implica dificultad de búsqueda, acceso e identificación, atento a que no se encuentran organizados o estructurados ni alfabéticamente ni por fecha de nacimiento, sino por fecha de celebración del bautismo. (artículo 4º, literal A) de la LPDP).

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

DICTAMINA:

1. Expedirse en el sentido expuesto en los considerandos I a III del presente.
2. Notifíquese, publíquese y oportunamente archívese.

m.j.r.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 2, de 22 de marzo de 2012.

Se dictamina sobre consulta formulada respecto a la redacción de una cláusula de confidencialidad a ser incorporada en el Fondo Concursable LA 21 de la Dirección Nacional de Empleo.

| DICTAMEN No. | | Expediente No. |
|--------------|------|-------------------|
| 2 | 2012 | 2012-2-10 0000097 |

Montevideo, 22 de marzo de 2012.

VISTO: La consulta formulada por el Ing. AA por la cual solicita al Órgano de Control, la redacción de una cláusula de confidencialidad a ser incorporada en el Fondo Concursable LA 21 correspondiente a “Servicios de desarrollo de software y migración de datos para el sistema “Vía Trabajo” de la Dirección Nacional de Empleo, utilizado por el INEFOP”, que se encuentra en ejecución.

RESULTANDO: I) Aduce que en el marco del referido proyecto, el proveedor necesita llevar una copia de la base de datos a su oficina para trabajar en la migración de los datos.

II) Manifiesta que se trata de una relación contractual requerida para el cumplimiento de la tarea encomendada: la migración; y que el registro de la base de datos respectiva, según han constatado, se encuentra en trámite.

III) Se expidió el informe jurídico N° 64, de 8 de febrero de 2012.

CONSIDERANDO: I) Que la situación en consulta se enmarca en una encargatura de tratamiento, siendo aplicable lo dispuesto por el artículo 14, inciso 2° del Decreto reglamentario N° 414/009, en tanto la tarea resulta necesaria para la prestación de un servicio al responsable.

II) Ello no obsta a que en razón de la tarea desarrollada, se deba dar cumplimiento con los principios consagrados en la Ley N° 18.331, esencialmente los de finalidad, reserva, seguridad y responsabilidad (artículos 8°, 10, 11 y 12 Ley N° 18.331, artículos 7° y 8°, Decreto N° 414/009).

III) En consecuencia, se sugiere la incorporación de una cláusula de confidencialidad, cuya redacción resulta del Informe N° 64/2012.

Dicha cláusula podrá ser aplicable en todas las tareas de migración, siempre y cuando éstas no posean características disímiles o particularizadas a la presente que ameriten un nuevo análisis por parte del Órgano de Control.

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

DICTAMINA:

1. Expedirse en el sentido expuesto en los considerandos I a III
2. Notifíquese, publíquese y oportunamente archívese.

m.j.r.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 3, de 29 de marzo de 2012.

Se dictamina sobre consulta formulada acerca de si existe obligación de registrar su base de datos de afiliados, por parte del Centro Integral del Personal de ANTEL (CIPA)

| DICTAMEN No. | | Expediente No. |
|--------------|-----|-------------------|
| 3 | 012 | 2012-2-10-0000229 |

Montevideo, 29 de marzo de 2012.

VISTO: La consulta formulada acerca de si existe obligación o no de registrar su base de datos de afiliados, por parte de uno de los sindicatos de ANTEL.

RESULTANDO: I) Que la referida base se compone por datos en papel y en formato electrónico, en ambos casos resguardados por la consultante.

II) Que asimismo incluye las direcciones electrónicas del padrón de afiliados y otras listas de interés, contenidas en la libreta de direcciones de las cuentas de ADINET que usan en sus comunicaciones.

CONSIDERANDO: I) Que el sujeto obligado al registro de una base de datos personales es aquél denominado por la ley como “responsable”, entendiéndose por tales no solamente a los propietarios de la base sino también a quien decida sobre la finalidad, contenido y uso del tratamiento.

II) Que la consultante cumple estos requisitos, ya sea porque su base de datos se compone de múltiples especies de datos personales además de las señaladas direcciones electrónicas, como por no estar ajena a decidir sobre la finalidad, contenido y uso de éstas una vez que las ingresa en su libreta de direcciones.

III) Que la situación planteada es la normal y frecuente en multiplicidad de casos donde se capturan o recolectan datos de una fuente preexistente, y no por ello se deja de hacer un tratamiento propio con tales datos deviniendo, en consecuencia, responsable para la ley.

IV) Que con respecto a la falta de funcionamiento del enlace <http://www.privacidad.adinet.com.uy> que informa la consultante, corresponde abrir expediente aparte para instruir y resolver sobre el punto.

ATENCIÓN: A lo precedentemente expuesto, al Informe del Asesor Letrado y a lo dispuesto por los arts. 4° lit. K), 28 29 y 34 D) de la Ley N° 18.331, de 11 de Agosto de 2008,

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

DICTAMINA:

1. Que existe obligación legal de inscribir la base de datos personales motivo de consulta, aunque la misma contenga direcciones de correos electrónicos provenientes de servidores ajenos a los consultantes.

2. Que atento a las resultancias de autos, corresponde disponer la apertura de nuevo expediente para instruir y resolver lo relativo a la falta de funcionamiento del enlace de Internet <http://www.privacidad.adinet.com.uy>

m.b.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 4, de 12 de abril de 2012.

Se dictamina sobre consulta formulada respecto a la celebración de un convenio de intercambio de datos entre la Intendencia de Canelones y Obras Sanitarias del Estado (OSE).

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 4 | 2012 | 2011-2-10-0000970 |

Montevideo, 12 de Abril de 2012.

VISTO: La consulta formulada respecto a la celebración de un Convenio de intercambio de conocimientos y datos entre la Intendencia de Canelones (IC) y Obras Sanitarias del Estado (OSE).

RESULTANDO: I) Que la IC brindará la información concerniente al nomenclator (numeración y calles), aspectos catastrales y toda otra relevante relativa a la georeferenciación de padrones del departamento y OSE la información de sus clientes: dirección, localidad, padrón, titular del contrato, tipo de documento (CI, Pasaporte, CC), número de documento, teléfono, email, relación con el servicio (propietario, inquilino, ocupante, etc.), dirección de envío, dirección de suministro.

II) Que en la cláusula séptima del borrador del convenio se establece que los datos obtenidos podrán publicarse en los distintos medios de difusión a fin de que tomen estado público y sean de fácil acceso para la población, verificándose previamente que no se revelen conocimientos, datos o información de carácter reservado de alguna de las partes.

CONSIDERANDO: I) Que respecto a la información a aportar por parte de la IC relativa a nombres de calles y números de padrones, en principio constituyen información pública siempre que esté dissociada de los titulares y por ende no presentaría objeciones desde el punto de vista de la protección de datos personales.

II) Que en cuanto a lo relativo al término “toda otra información relevante relativa a la georeferenciación de padrones del departamento de Canelones”, cabe tener presente que la Unidad ya se expidió en el Dictamen N° 6/2010, de 11 de febrero de 2010, respecto a que en las cédulas catastrales se encuentra el nombre de una persona relacionado con un determinado padrón, por lo que podría constituir un dato determinable de acuerdo a lo establecido en el artículo 4° de la LPDP, por lo cual deberá establecerse con claridad el alcance de este término en el convenio definitivo.

III) Que respecto a la información a aportar por parte de OSE, el art. 9° C) de la Ley N° 18.331 establece que no será necesario el previo consentimiento cuando los datos se encuentren en listados y se limiten en el caso de personas físicas a: nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento, lo cual indica que si

bien hay datos que no requieren previo consentimiento informado, hay otros que en cambio sí lo requieren como: número de Credencial Cívica, número de teléfonos fijos o celulares, emails y tipo de relación con el servicio (propietario, inquilino, ocupante, etc.).

IV) Que en definitiva, tanto la IC como OSE, deberán solicitar el consentimiento de los titulares para comunicar los datos que requieren el previo consentimiento informado.

V) Que para el caso de publicación o divulgación al público de dicha información, deberá estar en consonancia con lo establecido en las Leyes N° 18.331 de Protección de Datos Personales y N° 18.381 de Derecho de Acceso a la Información Pública (art. 10 Núm. II in fine).

ATENCIÓN: A lo dispuesto por los arts. 9°, 17 y 34 de la Ley N° 18.33, de 11 de agosto de 2008, El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1. Que IMC y OSE deberán obtener previamente el consentimiento informado del titular para intercambiar datos personales que no estén comprendidos en el listado establecido en el art. 9° C).

2. Que para publicar o difundir información que contenga dichos datos también se deberá recabar el consentimiento de los titulares o de lo contrario atender al carácter de información confidencial que poseen los mismos.

3. Notifíquese, publíquese.

g.r.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 5, de 13 de abril de 2012.

Se dictamina sobre consulta referida a la utilización de Identificadores de Objetos (OIDs) en el Ministerio de Relaciones Exteriores para identificar el ingreso de un usuario a la red.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 5 | 2012 | 2012-2-10-0000148 |

Montevideo, 13 de abril de 2012.

VISTO: La consulta referida a la utilización de OIDs en el Ministerio de Relaciones Exteriores para identificar el ingreso de un usuario a la red (logue) y la obligación de recabar el previo consentimiento informado.

RESULTANDO: I) Que para un mejor pronunciamiento de la Unidad se solicita a A/S Mauro Ríos la elaboración de un informe desde el punto de vista técnico.

II) Que en dicho informe se especifica que la identificación de personas mediante OIDs se construye con la Cédula de Identidad emitida por la Dirección Nacional de Identificación Civil o, -en el caso de un ciudadano de otro país-, con el documento de identificación aceptado por la Dirección Nacional de Migración, más el Código correspondiente al país.

III) Que el uso de un "OID de persona" bajo las especificaciones técnicas de la UNAOID para autenticarse ante un sistema informático, cumple la misma función que la definición de un usuario de dichos sistemas, por ende no aporta información per se respecto al mismo, más allá de su Cédula de Identidad, salvo que se implemente un sistema con ese objetivo.

CONSIDERANDO: I) Que el art. 9° Literal C) de la Ley N° 18.331 establece que no será necesario el previo consentimiento cuando se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento.

II) Que por tanto en este caso, la utilización del número de Cédula de Identidad o Pasaporte, así como el código del país que indica la nacionalidad, no exige recabar el previo consentimiento del titular para ser tratados.

III) Que además, respecto a la posibilidad de identificar a los usuarios en un sistema (logue), -ya sean funcionarios o interesados en trámites, etc., también puede aplicar el art. 9 B) que indica que no se requiere el previo consentimiento cuando los datos se recaben para el ejercicio de las funciones propias de los poderes del Estado o en virtud de una obligación legal.

IV) Que en caso de que la consulta refiera específicamente a los empleados o funcionarios como usuarios de la red, cabe también tener presente que existe una relación contractual, profesional o laboral entre los mismos y el organismo público, que lleva implícita la

posibilidad de éste de controlar si ingresan o no a la red (Art. 9 D), por cuestiones vinculadas al necesario control de la actividad y a la seguridad de la información.

ATENTO: A lo dispuesto por el art. 9° de la Ley N° 18.331, de 11 de agosto de 2008,

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

DICTAMINA:

1. Que no se requiere obtener el previo consentimiento informado para identificar a los usuarios de la red mediante la utilización de OIDs.

2. Notifíquese, publíquese.

g.r.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

Dictamen N° 6, de 4 de mayo de 2012.

Se dictamina la consulta formulada por el Carrasco Lawn Tennis Club, respecto de si resulta ajustado a derecho la entrega de datos personales que figuran en padrón social a requerimiento de sus socios.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|--------------------|
| 6 | 2012 | 2011-02-10-0000193 |

Montevideo, 15 de mayo de 2012.

VISTO: La ampliación de consulta formulada por Carrasco Lawn Tennis Club, respecto a si resulta ajustado a derecho la entrega de datos personales que figuran en su padrón social a requerimiento de sus socios, de acuerdo a lo que se establece en el art. 9° C) de la Ley.

RESULTANDO: Que se aduce que las solicitudes de los socios responden a diferentes motivos, entre otros para ser utilizados en actos electorales internos de la Institución tal como el que se celebrará próximamente.

CONSIDERANDO: I) Que la comunicación de datos que se pretende se encuentra regulada en el artículo 17 de la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP) y exige para su legitimidad la conjunción simultánea de los siguientes requisitos, el interés legítimo del emisor y del destinatario de la comunicación, y el previo consentimiento del titular de los datos, salvo las excepciones establecidas en la norma.

II) Que el art. 9° C) de la Ley establece que no será necesario el previo consentimiento cuando los datos se encuentren en listados y se limiten en el caso de personas físicas a: nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento.

III) Que de todas formas, aún en esta hipótesis, es necesario estar a lo establecido en los principios que inspiran la Ley, sobre todo al principio de finalidad (art. 8°) y al derecho de información (art. 13) que tienen los titulares cuyos datos serán comunicados.

IV) Que en referencia a los demás datos existentes en el padrón social, salvo la hipótesis que en los estatutos o en la ficha de afiliación se detalle expresamente la posibilidad de comunicación de datos a otros socios, para finalidades específicas, deberá recabarse el consentimiento informado del socio para legitimar la cesión.

ATENTO: A lo expuesto y a lo dispuesto por las normas legales citadas,

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

DICTAMINA:

1. Establecer que es ajustado a derecho comunicar los datos mencionados en el art. 9 C), con la finalidad de la realización del acto eleccionario e informando debidamente a los titulares.
2. Indicar a su vez, que no procede la comunicación de otros datos personales sin el consentimiento informado, salvo la hipótesis que dicho extremo resulte contemplado en los Estatutos o en la ficha de afiliación.
3. Notifíquese, publíquese y oportunamente archívese.

g.r.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 7, de 10 de mayo de 2012.

Se dictamina sobre consulta realizada por el Banco de Previsión Social (BPS) respecto si es suficiente la solicitud de turno o cita como forma de recabar el consentimiento para acceder a la historia clínica.

| DICTAMEN N° | | Expediente No. |
|-------------|------|-----------------|
| 7 | 2012 | 2011-2-10-00689 |

Montevideo, 10 de mayo de 2012.

VISTO: La consulta realizada por el Banco de Previsión Social (BPS).

RESULTANDO: I) Que la consulta refiere a si se considera suficiente la solicitud de turno o cita como forma de recabar el consentimiento respecto al acceso a la historia clínica por parte del usuario en la consulta médica, o si es necesario algún paso adicional en el encuentro clínico.

II) Que también hace referencia al Sistema Nacional de Certificación Laboral. El BPS informa que presta el subsidio por enfermedad. Para ello, en el marco del Sistema Nacional Integrado de Salud (SNIS) en los contratos de gestión que firmó la Junta Nacional de Salud (JUNASA) con los efectores de la salud, obliga a éstos, que tras la solicitud del trabajador, informen lo actuado al Instituto de Seguridad Social por medios electrónicos para que el trabajador pueda acceder al subsidio.

III) Que el expediente pasó a informe jurídico, el cual se realizó con fecha 20 de octubre de 2011.

CONSIDERANDO: I) Que de acuerdo con lo informado por el BPS se está ante la presencia de datos personales conforme con la definición contenida en el artículo 4° literal d) de la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP). Más específicamente, a datos de salud, los cuales son considerados datos sensibles, por lo que ninguna persona puede ser obligada a proporcionar este tipo de datos y sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular.

II) Que la LPDP indica que los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar datos personales relativos a la salud física o mental de los pacientes respetando los principios del secreto profesional, la normativa específica y lo establecido en la LPDP.

III) Que en relación con la primera consulta, se entiende que se recaba el consentimiento del titular cuando se realiza la llamada telefónica ya que la persona solicita determinado servicio, por lo que se está ante una manifestación de voluntad, libre, inequívoca e informada. Por tanto, a la hora de pedir la cita o turno se autoriza el acceso a los datos necesarios para realizar el tratamiento y no es necesario ningún otro requisito.

IV) Que la segunda consulta refiere a la legalidad de una comunicación de datos que se realiza entre el BPS, las instituciones médicas y los empleadores en el marco del Sistema Nacional de Certificación Laboral. Por tanto, se trata de una comunicación de datos conforme

con lo establecido en el artículo 4° literal b) de la LPDP y lo regulado por el artículo 17 de la misma norma.

V) Que en la presente consulta el consentimiento es prestado por el trabajador en el formulario que se transmite por medios electrónicos mediante su suscripción, por lo que se entiende que se está dando cumplimiento a este requisito. En cuanto al interés legítimo del emisor éste se verifica en que el trabajador desea acceder al subsidio por enfermedad. A su vez, el interés del destinatario radica en cumplir las funciones asignadas por Ley. Atento a ello, se considera que la comunicación de datos es legítima, cumpliéndose con todos los requisitos exigidos por la normativa vigente.

VI) Que el subsidio por enfermedad es un beneficio que abona BPS a los trabajadores activos, que por razones médicas se encuentran imposibilitados de trabajar de acuerdo con lo establecido en la Ley N° 14.407, del 22 de julio de 1975 y disposiciones concordantes. El Sistema Nacional de Certificación Laboral tiene como objetivo general aplicar un nuevo procedimiento de certificaciones médicas que permita consolidar la capacidad de gestión asociada al subsidio por enfermedad, rediseñando el modelo de atención en salud en el marco del Sistema Nacional Integrado de Salud.

VII) Que en el caso concreto resulta aplicable prima facie el artículo 17 de la LPDP, el que establece, por remisión al artículo 9 literal c) que no es necesario recabar el consentimiento cuando se trata de organismos en ejercicio de sus funciones. En este caso concreto, el BPS está ejerciendo una competencia propia asignada por Ley. En ese marco, la comunicación de datos que se realiza con las IAMC y con los empleadores quedaría amparada por esta excepción. Sin embargo, la consulta refiere a datos sensibles, será necesario – en definitiva - recabar el consentimiento expreso y escrito del titular, por lo que no se podría aplicar la anterior excepción. Se considera adecuado, que se obtenga el consentimiento de los titulares y la forma en que se recaba éste, así como revisar el alcance de la información que se solicita para ello.

ATENTO: A lo establecido en la LPDP y a lo precedentemente expuesto,
El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

1. Expedirse en el sentido de lo consignado en los Considerandos III a VII.
2. Notifíquese, y oportunamente publíquese.

f.b.

Fdo. Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen N° 8, de 15 de mayo de 2012.

Se dictamina sobre consulta proveniente de la Dirección Nacional de Hidrografía del Ministerio de Transporte y Obras Públicas (MTO), acerca de la adecuación de un sistema informático en desarrollo para la gestión de los puertos con la Ley N° 18.331.

| Dictamen No. | | Expediente No. | |
|--------------|-----|----------------|--------------|
| 8 | 012 | 2012 | 2-10-0000295 |

Montevideo, 15 de mayo de 2012.

VISTO: La consulta proveniente de la Dirección Nacional de Hidrografía del Ministerio de Transporte y Obras Públicas, acerca de la adecuación de un sistema informático en desarrollo para la gestión de los puertos, a la Ley N° 18.331.

CONSIDERANDO: El derecho de toda persona, sea pública como privada, a recibir asistencia y asesoramiento de la Unidad.

ATENCIÓN: A lo que surge del Informe de autos, y a lo dispuesto por el art. 34 lit. A) 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:

Téngase por evacuada la consulta en los términos que surgen del Informe Letrado N° 209, de 24 de abril de 2012, proporcionándose copia del mismo al consultante y sin perjuicio de las vías complementarias para continuar asesorándose, que enuncia el propio Informe.

m.b.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 9, de 24 de mayo de 2012.

Se dictamina sobre la consulta formulada por un integrante del Comité de Seguridad de la Información de la Agencia Nacional de Vivienda (ANV) respecto a la pertinencia y uso del correo electrónico entregado a los usuarios, así como la regulación de la privacidad de la información contenida en los mismos.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 9 | 2012 | 2012-2-10-0000296 |

Montevideo, 24 de mayo de 2012.

VISTO: La consulta formulada por un integrante del Comité de Seguridad de la Información de la Agencia Nacional de Vivienda, respecto a la pertenencia y uso del correo electrónico entregado a los usuarios, así como a la regulación de la privacidad de la información contenida en los mismos.

RESULTANDO: I) Que por tratarse de una consulta realizada por un integrante de un organismo público, se considerará que los términos “empresa” y “usuarios” refieren a organismo o administración y a empleados o funcionarios en el sentido amplio.

II) Que se realiza el correspondiente informe jurídico (Informe N° 201/2012).

CONSIDERANDO: I) Que respecto a la pertenencia del correo otorgado al trabajador, ya sea por una empresa u organismo público, es clara la jurisprudencia laboral en cuanto a considerar que es una herramienta y un recurso propio del empleador, entregado en tal carácter que cumpla con las tareas asignadas.

II) Que en razón de ello, se poseen ciertas potestades de control y de supervisión que habilitan a adoptar las medidas necesarias y proporcionales tendientes a salvaguardar la seguridad del sistema y el desarrollo adecuado de las actividades laborales.

III) Que respecto a la regulación de la privacidad de la información contenida en los mismos, en el Documento “Repertorio de recomendaciones prácticas de la OIT” (Ginebra, 1996), sobre la protección de la vida privada de los trabajadores se señala que el tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuaníme y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación laboral.

IV) Que de todas maneras, en referencia a la privacidad de la información contenida en los correos electrónicos institucionales (texto y encabezado de los mismos), no deberían contener información personal del trabajador en sentido estricto, por lo cual sería éste quien tiene la carga de usar esa herramienta sólo para el desempeño de tareas inherentes a su cargo.

V) Que no obstante ello, muchas veces contendrán información que atañe a la privacidad del trabajador, incluso datos sensibles que requieren una protección especial, como por ejemplo los datos de salud que deba comunicar el trabajador a su empleador.

VI) Que para ejercer el control, es necesario informar expresamente y por anticipado al trabajador, de manera expresa, precisa e inequívoca acerca del mecanismo que se utilizará, la finalidad que tiene y el alcance del mismo, ya sea mediante una circular o reglamento de circulación interna, salvo razones imperiosas que justifiquen continuar con la vigilancia encubierta cuando ésta proceda (art. 13 de la Ley N° 18.331).

VII) Que además, cada responsable de base de datos o de tratamiento de datos, está obligado a adoptar medidas de seguridad adecuadas para garantizar que los datos permanezcan seguros y confidenciales, evitando que sean modificados, consultados o tratados por terceros que no están autorizados para ello, y que por cualquier medio sean divulgados sin autorización (arts. 10, 11, 12, 18 y 19 de la Ley N° 18.331).

ATENCIÓN: A lo dispuesto en las normas antes citadas,

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

DICTAMINA:

1. Establecer que la administración pública y las empresas tienen derecho a controlar el uso de las cuentas de correo electrónico de su titularidad, limitándose en lo posible a los datos sobre tráfico más que al contenido en sí de las comunicaciones, salvo que ello sea necesario.
2. Indicar que se requiere informar expresamente y por anticipado al trabajador, así como utilizar los datos sólo para la finalidad para la cual han sido recabados, garantizando la seguridad y confidencialidad de los mismos.
3. Notifíquese, publíquese.

g.r.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 10, de 24 de mayo de 2012.

Se dictamina respecto a la consulta formulada por la Intendencia de Rocha respecto a la información solicitada por un Edil Departamental con relación a una Casa Refugio que atiende a personas en situación de calle.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 10 | 2012 | 2012-2-10-0000326 |

Montevideo, 24 de mayo de 2012.

VISTO: La consulta formulada por la Intendencia de Rocha respecto a la información solicitada por un Edil Departamental con relación a la Casa Refugio "AA" que atiende a personas en situación de calle.

RESULTANDO: I) Que en dicho pedido de informes se solicita información sobre la cantidad de personas que han ocupado el refugio desde el mes de octubre de 2011 a la fecha, así como el nombre completo de los ocupantes y su lugar de origen.

II) Que la Intendencia, frente a la posibilidad de informar la identidad de los beneficiarios del refugio manifiesta sus dudas, pues en el caso se contraponen el derecho que tiene el edil a solicitar determinada información, con el derecho a la protección de datos personales de esas personas, que además se encuentran en una especial situación de vulnerabilidad social.

CONSIDERANDO: I) Que respecto a la cantidad y origen de los ocupantes, al tratarse sólo de datos disociados de personas existentes en un determinado período de tiempo así como al lugar de donde provienen, no cabría realizar objeciones jurídicas.

II) Que en cuanto a la posibilidad de proporcionar sus nombres, corresponde considerar que el art. 1° de la Ley 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.

III) Que si bien el pedido de informes realizado por el edil se enmarca en lo establecido en el art. 284 de la Constitución, corresponde tener presente que estamos ante un derecho humano que posee un sistema de protección especial que también emana de nuestra Carta Magna.

IV) Que en definitiva corresponde equilibrar los distintos derechos e intereses en juego a la luz de los diferentes principios que guían la protección de datos personales, pero muy especialmente en base a los principios de finalidad y de proporcionalidad.

V) Que para comunicar ciertos datos personales, que por determinado motivo se encuentran en poder de un organismo público, indefectiblemente debe existir un juicio de proporcionalidad basado en la idoneidad, la necesidad y el equilibrio de los derechos en juego, y esto significa que debe existir una justificación que demuestre que es imprescindible la utilización de esa información, por ejemplo para investigar un delito, evitar un peligro eminente

o contribuir a determinada investigación judicial.

VI) Que la Ley recoge una serie de principios que delimitan las responsabilidades de quienes poseen y/o realizan tratamiento de datos personales, y deben 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).

VII) Que entre ellos, el de finalidad (art. 8°), verdadero pilar de la protección de datos personales, establece que los datos objeto de tratamiento no podrán utilizarse para finalidades distintas o incompatibles a aquellas que motivaron su obtención.

VIII) Que a su vez, el art. 7° contempla la necesidad de que el tratamiento y/o comunicación de un dato personal, sea proporcional a la finalidad que lo motiva, y en el caso, coincidiendo con lo expresado por la Intendencia, la comunicación de los nombres de los beneficiarios, no sólo vulneraría la protección de datos personales y la privacidad, sino la propia dignidad de estas personas.

IX) Que el Consejo Ejecutivo de la URCDP ya se ha expresado en tal sentido en el Dictamen N° 15 del 15 de setiembre de 2011 ante consulta presentada por el Fondo de Solidaridad, que respecto 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.

ATENCIÓN: A lo dispuesto en las normas antes citadas,

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

DICTAMINA:

1. Establecer que no caben objeciones jurídicas respecto a brindar al solicitante los datos relacionados con el lugar de origen y la cantidad de personas que han utilizado el refugio en dicho período.

2. Indicar que respecto a la identidad de esas personas, 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.

3. Notifíquese, publíquese.

g.r.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 11, de 31 de mayo de 2012.

Se dictamina sobre consulta realizada por los representantes del Nautilus Yachting sobre la comunicación de los datos del padrón electoral.

| DICTAMEN No. | | EXPEDIENTE No. |
|--------------|------|-------------------|
| 11 | 2012 | 2012-2-10-0000409 |

Montevideo, 31 de mayo de 2012

VISTO: La consulta realizada por los representantes del Nautilus Yachting sobre la comunicación de los datos del padrón eleccionario.

RESULTANDO: I) Que por informe jurídico N° 259 se establece que para la comunicación de los datos solicitados no requieren recabar el consentimiento de los titulares.

CONSIDERANDO: I) Que la URCDP, se ha pronunciado en casos similares, mediante el Dictamen N° 13/10 de 9 de junio de 2010 y el Dictamen 15/10, de 30 de julio de 2010, de los cuales surge que se podrán comunicar sin consentimiento los datos indicados en el literal C) del artículo 9°.

II) Que las bases de datos del Nautilus Yachting Club se encuentran inscriptas ante la URCDP, conforme al Decreto N° 414/2009.

ATENTO: A lo precedentemente expuesto y a lo dispuesto por la Ley N° 18.331,

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

1. INDICAR QUE PARA COMUNICAR LOS DATOS DEL PADRÓN ELECCIONARIO, ENUMERADOS EN EL LITERAL C DEL ARTÍCULO 9°, NO ES NECESARIO RECABAR EL CONSENTIMIENTO DE LOS TITULARES.

2. NOTIFÍQUESE Y PUBLÍQUESE.

r.i.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 12, de 7 de junio de 2012.

Se dictamina sobre consulta formulada por la Unidad de Acceso a la Información Pública (UAIP), respecto a la solicitud de información presentada ante la Intendencia de Montevideo y que contiene datos personales.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 12 | 2012 | 2011-2-10-0000955 |

Montevideo, 7 de junio de 2012.

VISTO: La consulta formulada por la Unidad de Acceso a la Información Pública (UAIP).

RESULTANDO: I) Que la solicitud de información pública presentada ante la Intendencia de Montevideo (IM), contiene datos personales como: N° Padrón, Propietarios, Domicilios y Datos (marca, modelo) de vehículos matrículas SBE AA, SBY BB (o BB), SBE CC.

II) Que por ello se solicita que el Consejo Ejecutivo de la URCDP se expida acerca de la pertinencia de entregar la referida información.

CONSIDERANDO: I) Que 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.

II) Que 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 Núm. II de la Ley N° 18.381.

III) Que respecto a la comunicación de datos personales, el artículo 17 de la Ley N° 18.331 (LPDP), 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.

IV) Que en el caso, dichos extremos no se verifican, ni las excepciones enunciadas en el artículo 17 para validar la comunicación de datos sin el previo consentimiento del titular, así como tampoco se cumplen los supuestos del artículo 9° al que remite el artículo 17 de la LPDP.

V) Por su parte, en el art. 4° de la Ley N° 18.331 se define "fuentes accesibles al público", indicando que son aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

VI) Que en el caso, existen normas limitativas (ambas leyes plantean el límite de la protección de datos personales) y además la finalidad de la base de datos de la IM, - tal como lo expresa el propio organismo-, no es la de un registro público que brinda información al público en general a cambio de una contraprestación, sino gestionar el cobro de la patente

vehicular tal como surge de la propia Constitución de la República (arts. 274 y 275) y a ello debe ajustarse el organismo .

VII) Que, por ende, la IM no puede solicitar a los particulares sus datos personales para entregarlos posteriormente en desmedro de la privacidad de los administrados, pues ello no se ajusta a los principios contenidos en la Ley N° 18.331, sobre todo al de Proporcionalidad y de Finalidad (arts. 7° y 8°).

VIII) Que en definitiva, sólo se podría brindar a los interesados toda información estadística relativa a la cantidad, tipo y marcas de vehículos que tributan en el departamento, sin incluir detalles que permitan identificar a los titulares, pues efectivamente en ese caso, se estaría vulnerando el art. 10 Num.II de la Ley N° 18.381 así como las disposiciones de la Ley N° 18.331 (arts. 1°, 5°, 7°, 8°, 9°, 11, 13 y 17).

ATENCIÓN: A lo dispuesto en las normas antes citadas,

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

DICTAMINA:

1.- Establecer 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.

2.- Notifíquese, publíquese.

g.r.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 13; de 28 de junio de 2012.

Se dictamina sobre la consulta formulada respecto al sistema de defunciones digital que se está implementando por parte del Ministerio de Salud Pública (MSP).

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 13 | 2012 | 2012-2-10-0000404 |

Montevideo, 28 de junio de 2012.

VISTO: La consulta formulada respecto al sistema de defunciones digital que actualmente está implantando el Ministerio de Salud Pública (MSP).

RESULTANDO: I) Que esto habilita a que los médicos certifiquen la defunción de una persona a partir del ingreso al sistema informático con su firma, al igual que lo hacen para el certificado de nacido vivo.

II) Que actualmente existe un web service que provee información de las defunciones certificadas por el MSP, al que sólo accede el Registro Civil, sin embargo otros organismos o entidades también han planteado el interés de acceder al mismo.

III) Que por ello es necesario conocer cuál es la restricción en materia de protección de datos personales, cuál es la validez legal que tiene el certificado electrónico del MSP sin la intervención del Registro Civil, cómo debe ser el esquema de funcionamiento de los organismos que requieren acceder a esta información y cómo debe formalizarse el acuerdo entre Registro de Estado Civil y MSP.

CONSIDERANDO: I) Que de acuerdo a lo previsto en los arts. 157 a 160 de la Ley N° 18.719, sobre intercambio de información entre Entidades Públicas, estatales o no, se deben adoptar todas aquellas medidas necesarias para promover el intercambio de información pública o privada, pero en este último caso con autorización del titular (o su representante) cuando así se requiera en la Ley N° 18.331.

II) Que en este sentido, el art. 158 de la Ley N° 18.719 establece que a los efectos del intercambio, una de las obligaciones consiste en recabar el consentimiento de acuerdo con lo previsto en la Ley N° 18.331, cuando el objeto de intercambio refiere a información privada o de particulares que requiere el previo consentimiento informado.

III) Que además, en el art. 159 se establece que dichas entidades deberán ajustar su actuación a una serie principios, entre ellos el de previo consentimiento informado, el de finalidad y el de confidencialidad y seguridad, los cuales a su vez, sirven de criterio interpretativo para resolver las cuestiones que puedan suscitarse.

IV) Que en el caso, un aspecto central a considerar es la finalidad del intercambio que deberá estar en consonancia con lo establecido en la Ley N° 18.331, por ello debe analizarse el marco de poderes y competencias que han sido asignadas por ley a cada organismo, para determinar si es posible aplicar algunas de las excepciones establecidas en la Ley antes mencionada.

V) Que en el caso, atento a los cometidos asignados al MSP en la Ley de su creación N° 9.202, de 12 de enero de 1934, y normas posteriores, así como al Registro Civil, por las

Leyes N° 13.737 (art. 154) y N° 14.269, y demás normas existentes, no es exigible recabar el consentimiento informado de los titulares de los datos, pues resulta aplicable el inciso B) del artículo 9°.

VI) Que no obstante ello, en el caso de que dicha comunicación se realice a otras entidades, como por ejemplo al BROU, se deberá recabar el previo consentimiento ya que los cometidos específicos de esta entidad no habilitan a interoperar directamente con el MSP, sino que corresponde que los datos de las defunciones de sus clientes sean proporcionados directamente por el Registro de Estado Civil.

VII) Que en cuanto a la confidencialidad de la causa de muerte, ésta se trata de un dato clínico reservado en virtud de lo dispuesto en la Ley N° 18.335 sobre Derechos de los Pacientes y Usuarios, así como en la Ley N° 18.331 de Protección de Datos Personales, y en este sentido la codificación de dicho dato clínico, es un mecanismo idóneo para garantizar la reserva y confidencialidad.

VIII) Que en cuanto a la validez de este certificado, debido a que la función del Registro de Estado Civil es anotar los hechos o actos que atañen al estado civil y sus registros hacen plena prueba y poseen la eficacia de los instrumentos públicos, dicho certificado deberá contar con la intervención del mismo, que podrá hacerlo a través del sistema con firma electrónica avanzada, tal como se dispone en la Ley N° 18.600 de Documento Electrónico y Firma Electrónica (art. 6°), a efectos de otorgarle la validez correspondiente.

IX) Que en cuanto al esquema de funcionamiento, los organismos involucrados podrán optar entre, celebrar un acuerdo de intercambio de información que establezca las condiciones, mecanismos y responsabilidades de cada uno o de lo contrario adoptar los mecanismos o condiciones definidas por la AGESIC y formalizar un acuerdo en base a ello.

ATENTO: A lo dispuesto en las normas antes citadas,

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

DICTAMINA:

1.- Establecer que en el caso resulta aplicable el inciso B) del artículo 9° que exime de recabar el previo consentimiento informado de los titulares, no obstante ello, esto no aplica en el caso de que dicha comunicación se realice a otras entidades que no posean estos cometidos específicamente establecidos por Ley como por ejemplo el BROU.

2. Indicar que los organismos podrán optar entre, celebrar un acuerdo de intercambio de información que establezca las condiciones, mecanismos y responsabilidades de cada uno; o de lo contrario adoptar los mecanismos o condiciones definidas por la AGESIC y formalizar un acuerdo en base a ello.

3. Precisar que en cuanto a la validez del certificado de defunción electrónico, éste deberá contar con la intervención del Registro de Estado Civil mediante el uso de la firma electrónica avanzada, a efectos de que posea la validez legal correspondiente.

4. Notifíquese, publíquese.

g.r.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 14, de 28 de junio de 2012.

Se dictamina respecto a la consulta formulada por el Instituto Nacional de las Mujeres-Departamento de las Mujeres Afrodescendientes del Ministerio de Desarrollo Social (MIDES), relativa a la formación e inscripción de una base de datos territorial de profesionales y/o técnicos de origen afrodescendientes.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 14 | 2012 | 2012-2-10-0000448 |

Montevideo, 28 de junio de 2012.

VISTO: La consulta formulada por el Instituto Nacional de las Mujeres (INMUJERES) - Departamento de las Mujeres Afrodescendientes, del Ministerio de Desarrollo Social (MIDES), sobre la formación e inscripción de una base de datos territorial de profesionales y/o técnicos de origen afrodescendiente.

RESULTANDO: I) Que dicho Departamento será el encargado de gestionar y recolectar los datos a través de un formulario digital auto-gestionado que se ubica en el sitio Web del MIDES, pero la gestión del espacio físico del soporte (el hosting y operación) de la Web MIDES la realiza la Empresa InnovaAge, mediante contrato celebrado con este ministerio.

II) Que el fundamento para la creación está en el mandato legal que se expresa en los Cometidos y Misión Institucional del MIDES y sus objetivos son fundamentalmente dos: a) obtener una base que sirva de justificación y fundamento para las Políticas Públicas, en especial las de Acción Afirmativa, y b) evaluar los posibles avances que se han producido en dichas políticas y su influencia en el colectivo afrodescendiente.

III) Que se consulta acerca de si es legítima o no la recolección y tratamiento de estos datos, -considerados datos sensibles-, por parte de este Departamento del MIDES, a la luz de lo establecido en el art. 18 de la Ley N° 18.331.

CONSIDERANDO: I) Que por regla, los datos de origen racial o étnico, -datos sensibles-, sólo pueden ser objeto de recolección y tratamiento con consentimiento expreso y escrito del titular o cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo (art. 18).

II) Que la especial tutela adjudicada a los datos sensibles, tiene por objeto evitar la discriminación, no obstante ello, también existe obligación de los Estados de actuar mediante políticas públicas adecuadas para favorecer el desarrollo de grupos y sectores de la sociedad que no tienen objetivamente las mismas posibilidades o propendiendo a la consolidación de una política social redistributiva de carácter progresivo, tal como se expresa en el DEC N° 286/006, de 22 de agosto de 2006.

III) Que por ello determinadas entidades públicas, de acuerdo con sus fines y cometidos, podrán mantener registro de este tipo de datos personales pues como en el caso, la finalidad

de la base es la justificación y fundamento para las Políticas Públicas que se adoptan, evaluar los avances que se han producido y su influencia en el colectivo afrodescendiente.

IV) Que además, atento a los cometidos asignados al MIDES por Ley de creación N° 17.866 y normas posteriores, no sería exigible recabar el consentimiento informado de los titulares, en tanto éstos sean efectiva o potencialmente beneficiarios de sus programas, por resultar de aplicación el inciso B) del artículo 9° de la Ley N° 18.331.

V) Que la referida base deberá ser inscripta en el Registro de la URCDP, en el plazo de 90 días desde su creación, así como contar con medidas de seguridad acordes.

ATENTO: A lo dispuesto en las normas antes citadas,

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

DICTAMINA:

1.- Establecer que se considera legítima la creación de la base referida a la luz de lo establecido en el art. 18 de la Ley N° 18.331.

2.- Indicar que deberá ser inscripta en el Registro de la URCDP dentro del plazo de 90 días contados desde la fecha de su creación, así como contar con medidas de seguridad acordes.

3.- Notifíquese, publíquese.

g.r.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen N° 15, de 2 de agosto de 2012.

Se dictamina sobre consulta formulada por el Fondo de Cesantía y Retiro de la Construcción (FOCER) relacionada a la comunicación de información que incluye datos personales de los beneficiarios.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 15 | 2012 | 2012-2-10-0000467 |

Montevideo, 2 de agosto de 2012

VISTO: La consulta formulada por el Fondo de Cesantía y Retiro de la Construcción (FOCER).

RESULTANDO: I) Que éste brinda una prestación a los trabajadores de la construcción en ocasión, de cese, retiro, o en casos extraordinarios, mediante un sistema de ahorro individual formado con aportes patronales y de los trabajadores.

II) Que la consulta refiere a la legalidad de la comunicación de datos personales que debe realizar FOCER a Cambio Gales Servicios Financieros SA y a Western Union, para efectuar el pago a trabajadores de nacionalidad argentina que gestionaron dicho beneficio pero luego se marcharon.

III) Que Cambio Gales expresa que para poder realizar los giros necesitan registrar a la empresa que remite los mismos, y además deben contar con un respaldo que explique el porqué de cada giro, ante la eventualidad de que el Banco Central les solicite esa información.

CONSIDERANDO: I) Que el artículo 17 de la Ley 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 en el caso evidentemente existe interés legítimo, tanto del emisor como del destinatario.

II) Que en lo que respecta al previo consentimiento el mismo artículo nos remite al art. 9° de la Ley, donde se establece que no será necesario cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

III) Que en este caso se trata de datos personales que constituyen un insumo para cumplir con las obligaciones que por ley se le asignan a las instituciones financieras, tanto por la Ley N° 17.835 sobre Sistema de Prevención y Control del Lavado de Activos y de la Financiación del Terrorismo, en su redacción dada por la Ley N° 18.494, como por su Decreto reglamentario, que imponen a los sujetos obligados el relevamiento, registro y conservación de datos personales de personas físicas y jurídicas.

IV) Que además, el art. 9 D) de la Ley establece otra excepción al consentimiento cuando los datos deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento, por lo cual en este caso los datos de los trabajadores deben ser comunicados para cumplir con las obligaciones surgidas en el marco de un contrato celebrado con FOCER.

V) Que en definitiva, si bien no existen impedimentos para dar curso a dicha comunicación

de datos en los términos establecidos en la consulta, es importante tener presente que aún respecto a aquellos datos que no requieren previo consentimiento informado, FOCER deberá observar los demás principios que estructuran la Ley, así como garantizar el ejercicio de los derechos consagrados en la misma.

ATENTO: A lo dispuesto en las normas antes citadas,

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

DICTAMINA:

1. Establecer que resultan aplicables las excepciones previstas en los incisos B) y D) del artículo 9° de la Ley N° 18.331 que eximen al consultante de recabar el previo consentimiento informado de los titulares.
2. Notifíquese, publíquese.

g.r.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 16, de 9 de agosto de 2012.

Se dictamina sobre consulta realizada por la Secretaría de la Cámara de Senadores acerca de la adecuación de las versiones taquigráficas de algunas actividades de la Cámara, a la Ley N° 18.331 y su Decreto reglamentario N° 414/009.

| DICTAMEN No. | | EXP. No. |
|--------------|----|-------------------|
| 16 | 12 | 2012-2-10-0000350 |

Montevideo, 9 de agosto de 2012.

VISTO: La consulta realizada por la Secretaría de la Cámara de Senadores acerca de la adecuación de algunas actividades de la Cámara a la Ley N° 18.331 y su Decreto reglamentario N° 414/009.

RESULTANDO: I) Que lo actuado en las sesiones y comisiones del Cuerpo, se recoge íntegramente en versiones taquigráficas de acuerdo con el art. 165 del Reglamento interno, las que actualmente se hacen públicas a través del sitio web del Parlamento.

II) Que estas versiones pueden contener datos personales susceptibles de protección, ante lo cual se consulta cómo proceder en estos casos sin vulnerar el derecho de acceso a la información pública, y si la Cámara tiene potestad para retirar todo o parte de la versión publicada en Internet.

III) Que otros aspectos consultados son:

- a) la determinación de un responsable de las bases de datos personales por cada una de las tres unidades ejecutoras que componen el Poder Legislativo;
- b) el valor más importante en caso de colisión de ambos derechos;
- c) el tratamiento de datos personales no contenidos en bases de datos;
- d) el tratamiento de bases informativas que además contienen datos personales.

CONSIDERANDO: I) Que el derecho de información incluyendo el de acceso a la información pública reconocido por la Ley N° 18.381, así como el derecho a la protección de los datos personales reconocido por la Ley N° 18.331, son derechos fundamentales que ingresan en la sistemática de interpretación y aplicación prevista por los arts. 7°, 72 y 332 de la Constitución.

II) Que en los casos de conflicto entre esos derechos, y aún en relación a otros valores de rango constitucional que no se resuelvan directamente en un derecho fundamental, se debe considerar a los derechos humanos como un sistema axiológico completo, en el cual todos ellos están llamados a coexistir de manera armónica.

III) Que desde el momento que el Poder Legislativo es un ámbito de la mayor trascendencia institucional en el cual es de esencia la libre participación y discusión de todo tipo de ideas y planteos, es necesario asegurar todas las vías posibles de comunicación y

publicidad de sus actividades, lo que de algún modo privilegia el derecho de información, y con ello la utilización de Internet como medio altamente aprovechable a tales efectos.

IV) Que no obstante lo expresado, no cabe afirmar una primacía absoluta del derecho de información en todas las situaciones, de manera que corresponderá a la autoridad responsable apreciar aquellos casos en los que -si se expusiera públicamente la información- podría quedar comprometido el derecho a la protección de datos personales.

V) Que si bien según el Reglamento del Senado se recoge la versión taquigráfica íntegra, ello no determina necesariamente su traslado a la red Internet, máxime cuando el propio Reglamento regula situaciones de reserva y además no existe norma expresa que ordene la utilización de este medio para todos los casos.

VI) Que existen enfoques y mecanismos concretos desarrollados por la doctrina especializada que facilitan la armonización perseguida, los que han sido reseñados en los Informes Letrados Nros. 344/2012 de este mismo expediente, y 6549/2011 del exp. N° 2011-2-10-0000334, y en la Res. N° 1442/2011 de la Unidad dictada en este último, a cuyas consideraciones la Unidad se remite.

VII) Que dada la estructura orgánica del Poder Legislativo, corresponde tener como “responsable de la base de datos” de que se trate al jerarca máximo de cada una de las tres Unidades Ejecutoras que lo componen: Cámara de Senadores, Cámara de Representantes y Comisión Administrativa.

VIII) Que el derecho a la protección de datos personales va más allá del soporte en el cual los datos estén registrados y tratados, por lo que su régimen jurídico se aplica también a datos personales que no forman parte de una base de datos, y a los contenidos en bases de datos de otro tipo.

ATENCIÓN: A lo precedentemente expuesto, a los arts. 7°, 72, 82 y 332 de la Constitución; 1°, 3°, 4° lit. K) y 24 de la Ley N° 18.331, de 11 de agosto de 2008; 4°, 9° y 10 de la Ley N° 18.381, de 17-10-2008; 23 lit. H) del Decreto N° 414/009 del Poder Ejecutivo, de 31 de agosto de 2009; 6°, 7°, 13, 25, 28, 29, 30 y 31 del Decreto N° 232/010 del Poder Ejecutivo, de 2 de agosto de 2010.

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

DICTAMINA:

1. Que en las situaciones de simultánea aplicación de los derechos a la protección de los datos personales, y el derecho de información -comprensivo del derecho de acceso a la información pública-, la competencia resolutoria por la autoridad responsable de la difusión de que se trate, la que deberá interpretar de manera armónica ambos derechos y, en su caso, procurar el menor sacrificio posible de aquéllos, según criterios expuestos en la parte expositiva del presente dictamen.

2. Que la Cámara de Senadores tiene atribuciones para retirar todo o parte de la versión

incorporada al sitio web cuando advierta que este tipo de difusión afecta algún valor constitucional esencial, o un derecho fundamental como es el derecho a la protección de los datos personales. En el ejercicio de esas atribuciones se estima pertinente prevenir tal circunstancia, evitando la publicación total o parcial en dicho medio.

3. Que la existencia de un responsable de datos diferente por cada unidad ejecutora del sistema orgánico Poder Legislativo, se adecua a lo que dispone la Ley N° 18.331.

4. Que también concuerda con el régimen jurídico vigente en materia de protección de datos personales, incluir en el mismo aquéllos datos no integrados a una base de datos, o que están incorporados en bases de datos que no son exclusiva o esencialmente de datos personales, todo ello sin perjuicio de un balance fundado a realizar en cada caso respecto a la aplicación de los derechos en cuestión.

m.b.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 17, de 16 de agosto de 2012.

Se dictamina sobre la consulta presentada por el Ministerio de Educación y Cultura (MEC), Dirección General de Registro de Estado Civil (DGR), respecto a las solicitudes de acceso que recibe de parte de organismos públicos y privados, respecto a la información contenida en sus bases de datos.

| DICTAMEN N° | | Expediente No. |
|-------------|-----|-------------------|
| 17 | 012 | 2011-2-10-0000586 |

Montevideo, 16 de agosto de 2012

VISTO: La consulta presentada por el Ministerio de Educación y Cultura, Dirección General de Registro de Estado Civil.

RESULTANDO: I) Que la consulta refiere a las solicitudes de datos que recibe la Dirección General de Registro de Estado Civil por parte de organismos públicos y privados respecto a la información contenida en sus bases de datos.

II) Que específicamente se consulta acerca de si se encuentran habilitados para entregar la información y con qué alcance

CONSIDERANDO: I) Que se está ante datos personales contenidos en las bases llevadas por la Dirección General de Registro de Estado Civil y que se regulan por el Decreto-Ley N° 1.430, de 12 de febrero de 1879.

II) Que respecto a la aplicación de la Ley N° 18.331, de 11 de agosto de 2008, debe tenerse presente lo dispuesto por su artículo 3° literal C), en cuanto a su ámbito objetivo de aplicación, del cual se excluye a las bases de datos creadas y reguladas por leyes especiales, situación en la que se encuentra la base considerada.

III) Que según lo dispuesto por los artículos 9° y 17 de la Ley citada, relativos al consentimiento del titular de los datos personales, éste no será necesario cuando los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de información.

IV) Que sin perjuicio de lo expuesto, corresponde tener presente que la Ley 18.331 configura el régimen general en el derecho positivo actual en materia de protección de datos personales, como derecho inherente a la persona humana comprendido en el artículo 72 de la Constitución de la República.

V) Que por el mismo, al resolver sobre la entrega de la información a los posibles solicitantes, la consultante debe ajustar sus decisiones a los principios fundamentales en materia de protección de datos personales. Por ello, no es posible que la información contenida en sus bases de datos sea comunicada en forma excesiva o indiscriminada, lo cual podría

violentar los derechos de las personas; en cada caso procede atender la pertinencia de la respectiva solicitud y la finalidad para la cual se requieren los datos.

ATENTO: A lo establecido en la LPDP y a lo precedentemente expuesto,

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

DICTAMINA:

1. Establecer que no resulta aplicable a las bases de datos llevadas por la Dirección de Registro de Estado Civil el régimen de la Ley N° 18.331 de 11 de agosto de 2008.
2. Indicar que igualmente esa Dirección deberá atender a los principios generales de la protección de datos personales a los efectos de resolver sobre las solicitudes de información que obre en sus bases.
3. Notifíquese, y oportunamente publíquese.

j.h.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 18, de 30 de agosto de 2012.

Se dictamina sobre consulta realizada por la Asesoría Letrada de la Dirección General de Registro (DGR) en relación con publicación en la página web, de las resoluciones administrativas.

| DICTAMEN No. | | EXPEDIENTE No. |
|--------------|------|-------------------|
| 18 | 2012 | 2012-2-10-0000560 |

Montevideo, 30 de agosto de 2012.

VISTO: La consulta realizada por la Asesoría Letrada de la Dirección General de Registro (DGR), consulta a la URCDP sobre la publicación en la página web de las resoluciones administrativas.

RESULTANDO: Que según lo expresado la DGR consulta si puede publicar en su página web las resoluciones administrativas derivadas de peticiones o derivadas de contenciosos administrativos, con la finalidad de dar a conocer la posición de la DGR en las diferentes materias.

CONSIDERANDO: I) Que la URCDP está facultada a asesorar sobre el alcance de la Ley N° 18.331, de acuerdo a lo establecido en el art. 34. de la precitada norma.

II) Que la Dirección Nacional de Registros cuenta con una ley especial de creación y regulación, la Ley N° 16.871, por lo que entra dentro de la excepción planteada en al literal C) de la Ley N° 18.331.

III) Respecto al consentimiento previo e informado que establecen los artículos N° 9° y 17, no es necesario recabar si los datos provienen de fuentes públicas tales como registros públicos.

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

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

DICTAMINA:

1. HACER SABER A LA DIRECCION GENERAL DE REGISTROS EL CRITERIO QUE SURGE DE LA PARTE EXPOSITIVA DEL PRESENTE DICTAMEN.

2. NO OBSTANTE LO ANTERIOR, SE RECOMIENDA A LA CITADA DIRECCIÓN TRATAR LOS DATOS PERSONALES DE ACUERDO CON LOS PRINCIPIOS GENERALES APLICABLES EN LA MATERIA Y, ESPECÍFICAMENTE EN LO RELATIVO A LA PUBLICACIÓN EN LA PÁGINA WEB A QUE REFIERE LA CONSULTA DE OBRADOS EFECTUAR UN PROCESO DE DISOCIACIÓN.

3. NOTIFÍQUESE Y PUBLÍQUESE.

r.i.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 19, de 6 de setiembre de 2012.

Se dictamina sobre la consulta referida a las eventuales consecuencias jurídicas que tendría contratar el servicio de videovigilancia ofrecido por la Administración Nacional de Telecomunicaciones (ANTEL), que permite instalar una cámara en la cocina-comedor del domicilio particular donde cumple funciones la niñera.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 19 | 2012 | 2011-2-10-0000818 |

Montevideo, 6 de setiembre de 2012.

VISTO: La consulta referida a las eventuales consecuencias jurídicas que tendría contratar el servicio de videovigilancia ofrecido por ANTEL, (<http://www.antel.com.uy/antel/personas-yhogares/movil/servicios/con-costo/Video-vigilancia>), a efectos de instalar la cámara en la cocina-comedor del domicilio particular donde realiza su tarea la niñera contratada para el cuidado de los hijos menores de edad.

RESULTANDO: I) Que el servicio de ANTEL refiere a un sistema de vigilancia y seguridad para el hogar, la oficina o el comercio a través del cual se puede monitorear en tiempo real desde el PC, laptop o celular.

II) Que el consultante pretende contratar este servicio para monitorear el ámbito de su hogar, concretamente la cocina- comedor del mismo, que si bien es considerado como ámbito doméstico, no sería tal para la persona que desempeña funciones cuidando a sus hijos menores de edad.

CONSIDERANDO: I) Que la evolución producida en materia de derecho a la intimidad y a la privacidad, ha llevado a que el “derecho a estar solo” adquiera una dimensión más social y colectiva, llegándose así al derecho a tener el control y protección adecuada de los datos personales, por lo cual corresponde analizar aquellos casos, -como éste-, donde se entrecruzan varios derechos de raigambre constitucional, desde una perspectiva que enfatice en esta nueva concepción.

II) Que de acuerdo con 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, entre los principios generales se señala que el tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuaníme y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación de empleo del trabajador.

III) Que por otra parte la Guía de INTECO sobre Videovigilancia y PDP en su sección “Control laboral en entornos domésticos”, establece que “es legítima la utilización de cámaras en entornos domésticos para el control laboral de personas ajenas contratadas, por ejemplo para el desempeño de tareas de mantenimiento, cuidado de niños o cualquier otro servicio

prestado en el interior del domicilio”.

IV) Que no sería necesario obtener el consentimiento de la persona afectada por el sistema de videovigilancia pues el art. 9 de la Ley N° 18.331 establece una serie de excepciones entre las cuales encontramos en el Numeral D), que si esos datos derivan de una relación contractual y son necesarios para su desarrollo o cumplimiento de la misma, no se exige recabar dicho consentimiento en forma expresa. En el caso analizado, puede considerarse que este tratamiento es necesario para el adecuado desenvolvimiento de la relación laboral referida al cuidado de los niños.

V) Que sin perjuicio de lo anterior, la instalación de cámaras tendrá que respetar los demás requisitos exigidos por la legislación vigente en la materia, especialmente el deber de informar expresamente y en forma anticipada a la trabajadora pues de esta forma la videovigilancia pasa a formar parte de la propia relación laboral y el tratamiento de los datos pasa a ser necesario para el adecuado desenvolvimiento de la misma (art. 13 de la Ley N° 18.331).

VI) Que las imágenes sólo pueden ser utilizadas para la finalidad para la cual han sido recabadas (art. 8° de la Ley N° 18.331), así como 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.

VII) Que también deberán respetarse los espacios privados de la trabajadora (baños, dormitorios o vestuarios), pues la videovigilancia en estos casos afecta su 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° núm. 2 de la Ley N° 18.331), así como garantizar la seguridad y confidencialidad de las imágenes que se obtienen (art.11 de la Ley N° 18.331).

ATENCIÓN: A lo dispuesto por los arts. 1°, 6° Numeral 2°, 8°, 9° Numeral D), 11, 13 y demás pertinentes de la Ley N° 18.331 de 11 de agosto de 2008;

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

DICTAMINA:

1. Que no sería necesario obtener el consentimiento de la persona afectada por el sistema de videovigilancia de acuerdo a lo establecido en el art. 9° de la Ley N° 18.331 Numeral D).
2. Que a efectos de cumplir con la ley deberá estarse a las demás exigencias indicadas.
3. Notifíquese, publíquese.

g.r.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 20, de 6 de setiembre de 2012.

Se dictamina sobre consulta realizada por Nalistar S.A. relativa a si corresponde una cláusula en un contrato de adhesión.

| DICTAMEN No. | | EXPEDIENTE No. |
|--------------|------|-------------------|
| 20 | 2012 | 2012-2-10-0000453 |

Montevideo, 6 de setiembre de 2012.

VISTO: La consulta realizada por Nalistar S.A. relativa a si corresponde una cláusula en un contrato de adhesión.

RESULTANDO: Que por informe jurídico se recomienda a la Asociación de Respuesteros de Automotores del Uruguay la consideración de los principios legales en el tratamiento de datos personales.

CONSIDERANDO: I) Que de acuerdo al artículo 9° de la Ley N° 18.331, no sería necesario el previo consentimiento informado, en la autorización a la Asociación de Respuesteros Automotores del Uruguay para la búsqueda de la misma en la Dirección Nacional de Aduanas (DNA), a través de la Cámara Nacional de Comercio y Servicios del Uruguay (CNyS) o Liga de Defensa Comercial (LIDECO), atento a que existe una obligación legal pautada por la Ley N° 17.849.

II) Que la nueva cláusula referida a las responsabilidades de la Asociación de Respuesteros Automotores del Uruguay por el manejo de datos personales es conteste con la normativa de Protección de Datos Personales.

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

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

DICTAMINA:

1. RECOMENDAR A LA ASOCIACIÓN DE RESPUESTEROS AUTOMOTORES DEL URUGUAY TOMAR EN CONSIDERACIÓN LOS PRINCIPIOS DE LA LEY N° 18.331.
2. INDICAR QUE NO ES NECESARIO EL PREVIO CONSENTIMIENTO INFORMADO EN LA AUTORIZACIÓN A LA ASOCIACIÓN DE RESPUESTEROS AUTOMOTORES DEL URUGUAY PARA LA BÚSQUEDA DE LA MISMA EN LA DIRECCIÓN NACIONAL DE ADUANAS (DNA), A TRAVÉS DE LA CÁMARA NACIONAL DE COMERCIO Y SERVICIOS DEL URUGUAY (CNYS) O LIGA DE DEFENSA COMERCIAL (LIDECO).
3. NOTIFÍQUESE Y PUBLÍQUESE.

r.i.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 21, de 20 de setiembre de 2012.

Se dictamina sobre consulta realizada por la Administración de las Obras Sanitarias del Estado (OSE), respecto a si procede comunicar datos de funcionarios y sus cónyuges al Servicio de Garantía de Alquileres de la Contaduría General de la Nación.

| DICTAMEN No. | | EXPEDIENTE No. |
|--------------|------|-------------------|
| 21 | 2012 | 2012-2-10-0000469 |

Montevideo, 20 de setiembre de 2012.

VISTO: La consulta realizada por la Administración de las Obras Sanitarias del Estado (OSE) sobre si procede comunicar datos de funcionarios y sus cónyuges al Servicio de Garantía de Alquileres de la Contaduría General de la Nación (CGN).

RESULTANDO: Que en el presente caso se plantea una comunicación de datos, la cual es procedente para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.

CONSIDERANDO: I) Que la comunicación de datos exige interés legítimo del emisor y del destinatario y previo consentimiento del titular de los datos, para realizarse conforme a la Ley N° 18.331.

II) Que conforme al artículo 5° del Decreto N° 414/2009 establece que el titular deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos, y el tipo de actividad desarrollada por el responsable de la base de datos o tratamiento. En caso contrario, el consentimiento será nulo.

III) Que de acuerdo a la Ley y al Decreto mencionados, las bases de datos personales de OSE deben ser inscriptas ante la URCDP.

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

DICTAMINA:

1. ESTABLECER QUE LA CONTADURIA GENERAL DE LA NACIÓN DEBERÁ RECABAR LOS DATOS REFERIDOS A LOS CÓNYUGES DE LOS FUNCIONARIOS QUE SOLICITE EL SERVICIO DE GARANTÍA DE ALQUILERES, Y NO EL ORGANISMO AL QUE PERTENECEN LOS SOLICITANTES (EN ESTE CASO LA ADMINISTRACIÓN DE LAS OBRAS SANITARIAS DEL ESTADO).

2. INDICAR QUE OSE PODRÁ RECOLECTAR LOS DATOS DE LOS CÓNYUGES, CON SU CONSENTIMIENTO, PARA SER COMUNICADOS A LA CONTADURÍA GENERAL DE LA NACIÓN.

3. INDICAR ASIMISMO QUE OSE DEBERÁ INSCRIBIR EN CARÁCTER DE RESPONSABLE, LAS BASES DE DATOS PERSONALES QUE ADMINISTRA.

4. NOTIFÍQUESE Y PUBLÍQUESE.

r.i.

Fdo. Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen N° 22, de 4 de octubre de 2012.

Se dictamina la consulta formulada por la Secretaría General de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) relativa a la adecuación de determinados aspectos del pliego de licitación del sistema de denuncia en línea del Ministerio del Interior (MI).

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 22 | 2012 | 2012-2-10-0000679 |

Montevideo, 4 de octubre de 2012.

VISTO: La consulta formulada por Secretaría General de AGESIC acerca de la adecuación de determinados aspectos del pliego de licitación del sistema de denuncia en línea del Ministerio del Interior.

RESULTANDO: Que se solicita la opinión del Consejo acerca del formulario elaborado para recabar el consentimiento para el tratamiento de los datos personales de los involucrados, y si además es necesario que se recabe el consentimiento del personal que ha sido contratado por el oferente, mediante la firma de los titulares en su respectivo currículum o por carta complementaria.

CONSIDERANDO: I) Que respecto al primer aspecto de la consulta no se presentan objeciones en relación a los puntos señalados en el formulario, salvo recomendar que se elimine la expresión “cualquier forma de...”, quedando redactado de la siguiente manera: “...manifiesta que consiente la utilización, comunicación...”.

II) Que en cuanto al segundo aspecto, cabe tener presente que la URCDP ya se ha expedido respecto a este tema en consulta similar, mediante el Dictamen N° 17/010, de 20 de agosto de 2010 (Expediente N° 009/2010).

III) Que conforme al artículo 9° de la LPDP, la persona que se postula a un llamado laboral y entrega su Curriculum Vitae a su empleador, ya está prestando su consentimiento de forma documentada, libre, previa, expresa e informada, lo que incluye las tareas a desarrollar en el marco de una licitación como la presente, estando ello en consonancia con el principio de finalidad establecido en el artículo 8 de la LPDP.

IV) Que también debe considerarse lo expresado en el artículo 17 que 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, el cual no será necesario en una serie de excepciones, por ejemplo en la prevista en el art. 9° D) de la Ley o sea cuando los datos “deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento”.

V) Que en definitiva, considerando lo ya expresado por la URCDP en anterior dictamen

y analizando las circunstancias planteadas en la consulta, cabe concluir que no sería necesario recabar el previo consentimiento sin perjuicio de que dichos oferentes tienen el deber de informar a quienes se incluyen en la licitación, en los términos establecidos en el art. 13 de la Ley.

VI) Que respecto a las obligaciones del organismo que debe controlar los pliegos de condiciones de las licitaciones, se debe considerar que no corresponde el control de tal requisito, pues ello es parte de las obligaciones que poseen los responsables de las bases de datos o del tratamiento de los datos personales de los trabajadores con quienes mantienen el vínculo laboral.

ATENCIÓN: 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 el formulario elaborado por AGESIC se adecua a la normativa de protección de datos personales, sin perjuicio de que se estima conveniente la eliminación de la expresión señalada en el Considerando I.
2. Establecer que no es necesario que se recabe, por parte del oferente, el consentimiento del personal a su cargo, salvo la obligación de informar en los términos del art. 13 de la Ley.
3. Señalar que no corresponde el control de la existencia de dicho consentimiento por parte del organismo encargado de la revisión del pliego de la licitación.
4. Notifíquese, publíquese.

g.r.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 23, de 4 de octubre de 2012.

Se dictamina sobre consulta realizada por la Dirección de Epidemiología del Ministerio de Salud Pública (MSP) respecto a la regulación de las bases de las cuales es responsable.

| DICTAMEN N° | | Expediente No. |
|-------------|-----|-------------------|
| 23 | 012 | 2012-2-10-0000668 |

Montevideo, 04 de octubre de 2012.

VISTO: La consulta presentada por la Dirección de Epidemiología del Ministerio de Salud Pública respecto a las bases de datos de las cuales es responsable.

RESULTANDO: I) Que la consulta refiere a la aplicación de la Ley N° 18.331, de 11 de agosto de 2008, a las bases de datos relativas a la mortalidad, natalidad, información perinatal y enfermedades de notificación obligatoria de las cuales es responsable.

II) Que el expediente pasó a informe jurídico, el cual se realizó con fecha 27 de agosto de 2012.

CONSIDERANDO: I) Que se está ante bases de datos que contienen datos personales de naturaleza sensible, los cuales se encuentran especialmente protegidos por la Ley N° 18.331.

II) Que al tratarse de datos de esa naturaleza, la ley exige como principio general, que para su tratamiento o comunicación se cuente con el consentimiento expreso y escrito de su titular, admitiéndose excepciones previstas expresamente en la Ley.

ATENTO: A lo expuesto al Informe Letrado N° 414, de 27 de agosto de 2012, a lo establecido en la LPDP y a lo precedentemente expuesto,

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

DICTAMINA:

1. Expedirse en cuanto a las consultas formuladas en los términos que surgen del Informe N° 414, de fecha 27 de agosto de 2012, emitido por esta Unidad, el cual se incorpora como parte del presente Dictamen.

2. Notifíquese, y oportunamente publíquese.

j.h.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 24, de 4 de octubre de 2012.

Se dictamina sobre consulta formulada por la Unidad de Acceso a la Información Pública (UAIP) respecto al carácter que poseen determinados datos personales que se incluyen en una solicitud de acceso presentada ante el Ministerio de Relaciones Exteriores (MREE).

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|------------------|
| 24 | 2012 | 2012-6-1-0003979 |

Montevideo, 4 de octubre de 2012.

VISTO: La consulta formulada por la Unidad de Acceso a la Información Pública (UAIP), respecto al carácter que poseen determinados datos personales que se incluyen en una solicitud de acceso a la información pública presentada ante el Ministerio de Relaciones Exteriores (MRREE).

CONSIDERANDO: I) Que los datos refieren a los empleados o personal contratado, nacional o extranjero, que prestan funciones como Secretarios, Cancilleres y Oficiales de Cancillería (art. 17 del Decreto N° 462/995), Cancilleres y Auxiliares Administrativos (Art. 5 del Decreto N° 230/974). No se incluye el personal contratado de servicio (personal de seguridad, chofer, etc.), tampoco al personal que cumple funciones para los cónsules honorarios.

II) Que lo que se solicita refiere a: tipo de función (ejemplo auxiliar administrativo), representación donde desempeña funciones (ejemplo Consulado General de Barcelona), nacionalidades (ejemplo uruguayo y español), fecha de nacimiento, fecha de inicio de funciones en la representación, número de años completos en funciones, partida de contratación asignada (total en moneda local y conceptos incluidos: (sueldo neto, aportes empleador/empleado, impuesto a la renta), fecha de última modificación -ajustes por inflación, aumentos de sueldo.

III) Que se considera que los datos referidos al tipo de función, representación, fecha de inicio de funciones y número de años completos en funciones, -datos que en definitiva hacen al rol que cada funcionario cumple para y en la actividad pública-, deben ser considerados públicos sin más análisis, aunque es cometido atribuido legalmente a la UAIP determinar en última instancia tal carácter, en base a lo establecido en la Ley N° 18.381 y su Decreto Reglamentario.

IV) Que los datos relativos a la nacionalidad y fecha de nacimiento de estos funcionarios, deben ser incluidos dentro de lo previsto en el art. 9° C) de la Ley N° 18.331, por lo tanto para su tratamiento no se requiere el previo consentimiento informado.

V) Que por último, respecto a los datos que refieren a los ingresos de estos funcionarios o sea la partida de contratación asignada (total en moneda local y conceptos incluidos: sueldo neto, aportes empleador/empleado, impuesto a la renta, fecha de última modificación -ajustes por inflación, aumentos de sueldo), corresponde realizar la prueba o test del interés público, lo que implica interpretar y en definitiva aplicar las disposiciones contenidas en la Ley N° 18.381

y su Decreto Reglamentario N° 232/2010, actividad que se entiende inmanente al Órgano de Control designado a tales efectos, o sea a la Unidad de Acceso a la Información Pública.

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 los datos relativos a la nacionalidad y fecha de nacimiento de estos funcionarios, de acuerdo a lo previsto en el art. 9 C) de la Ley N° 18.331, no requieren para su tratamiento el previo consentimiento informado.

2. Señalar que respecto de los otros datos contenidos en la solicitud de obrados, la cuestión concierne directa y específicamente a la Unidad de Acceso a la Información Pública.

3.- Notifíquese, publíquese.

g.r.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 25, de 12 de octubre de 2012.

Se dictamina sobre consulta formulada respecto a los casos de interoperabilidad o intercambio de información entre organismos públicos (artículo 157 Ley N° 18.719), que implican comunicación de datos personales y la aplicación de la excepción del literal b) del artículo 9 de la Ley N° 18.331.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 25 | 2012 | 2012-2-10-0000687 |

Montevideo, 12 de octubre de 2012.

VISTO: La consulta formulada en obrados respecto a si en los casos de interoperabilidad o intercambio de información entre Organismos Públicos (art. 157 de la Ley N° 18.719), que implican comunicación de datos personales y donde aplica la excepción del literal b) del art. 9° (al cual remite el art.17), ello también implica el relevo del control de los fines vinculados con el interés legítimo (art. 17) o solo refiere al consentimiento. Formula la misma consulta para cuando opera la excepción del literal c) del art. 9° en referencia al control del interés legítimo. CONSIDERANDO: I) Que el art. 158 de la Ley N° 18. 719, de 27 de diciembre de 2010, establece que a los efectos del intercambio de información entre Entidades Públicas, estatales o no, una de las obligaciones consiste en recabar el consentimiento, de acuerdo con lo previsto en la Ley N° 18.331, cuando el objeto de intercambio refiere a información privada o de particulares que requiere el previo consentimiento informado.

II) Que el art. 159 establece que las Entidades Públicas deberán ajustar su actuación a una serie de principios, como por ejemplo el de previo consentimiento informado, el de finalidad, el de confidencialidad y seguridad, por lo cual, aún respecto a aquellos datos que no requieren previo consentimiento informado, también se deberán observar el resto de los principios que estructuran la Ley N° 18.331.

III) Que debido a ello, cuando se intercambia determinada información entre organismos debe considerarse especialmente el marco de poderes y competencias que le han sido asignadas legalmente a cada uno de ellos, a efectos de determinar si es posible o no aplicar algunas de las excepciones establecidas en la Ley.

IV) Que en definitiva, aunque no sea necesario recabar el consentimiento sí deberá atenderse a la finalidad, al marco legal y a los cometidos de cada organismo interviniente, las cuales deben corresponderse con el interés que subyace, tanto en las gestiones que atañen a los propios usuarios, como en los servicios que debe brindar el Estado para cumplir con sus funciones.

V) Que para complemento de lo anterior se considera que el art. 159 de la Ley N° 18.719, establece un marco de actuación cuyo procedimiento debe ser iniciado con la presentación de una solicitud fundada y firmada por el jerarca del organismo emisor, ante el jerarca del

organismo receptor, y que los acuerdos además deberán establecer las condiciones, protocolos y criterios funcionales o técnicos con los que se llevarán a cabo dichos intercambios, todo lo cual debe ser interpretado como parte del control de la finalidad y el interés legítimo, más allá de que no se requiera obtener el previo consentimiento informado en las hipótesis previstas en la Ley N° 18.331 art. 9° B) y C).

ATENCIÓN: 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 si bien en los casos comprendidos dentro de las excepciones, no debe recabarse el previo consentimiento informado, sí deberá atenderse a la finalidad e interés legítimo, así como a los cometidos específicamente establecidos por Ley a los organismos intervinientes.

2.- Notifíquese, publíquese.

g.r.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 26, de 1 de noviembre de 2012.

Se dictamina sobre la consulta formulada respecto a cómo adecuar el contenido de las resoluciones del Directorio de la Administración de las Obras Sanitarias del Estado (OSE) de acuerdo con lo establecido en la Ley N° 18.331 a efectos de que sean publicadas en la web de dicho organismo.

| DICTAMEN N° | | EXPEDIENTE N° |
|-------------|------|-------------------|
| 26 | 2012 | 2012-2-10-0000435 |

Montevideo, 1 de noviembre de 2012.

VISTO: La consulta formulada en estos obrados respecto a cómo adecuar el contenido de las Resoluciones del Directorio de la Administración de las Obras Sanitarias del Estado (en adelante OSE), a lo establecido en la Ley N° 18.331 de Protección de Datos Personales, con la finalidad de ser publicadas en la web de dicho organismo público.

RESULTANDO: I) Que se solicita que el Consejo Ejecutivo de la URCDP se expida acerca de determinados criterios que permitan la publicación de dichas resoluciones sin vulnerar el derecho a la protección de datos personales.

II) Que corresponde tener presente que no hay soluciones uniformes y globales que puedan abarcar la universalidad de hipótesis que puedan plantearse en cada organismo público.

CONSIDERANDO: I) Que hay datos que deben ser resguardados pues se trata de datos personales que requieren previo consentimiento informado según se establece en la Ley N° 18.331 y el art. 10 Núm. II de la Ley N° 18.381.

II) Que en aras de proteger la dignidad de aquellas personas sometidas a un sumario administrativo, el expediente podría ser clasificado como reservado de acuerdo con el art. 9° D) de la Ley N° 18.381, y dicha reserva debería durar hasta tanto se resuelva definitivamente sobre el asunto, brindándose luego acceso a la resolución que corresponda.

III) Que en cuanto a la publicación en la web, según lo establecido en la Ley N° 18.331 art. 9°, existen determinados datos personales que no requieren el previo consentimiento para ser tratados, respecto a las personas físicas los 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.

IV) Que por otra parte, el literal b) del artículo 9° establece que no es 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”, por lo cual en este caso es razonable interpretar que la Ley N° 18.381 de Acceso a la Información Pública contiene una obligación legal que tiene como objetivo garantizar la transparencia de la administración pública.

V) Que además, de acuerdo con la Ley N° 18.331 hay 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.

VI) Que de todas maneras, corresponde analizar ante el caso concreto, si el contexto no revela directa o indirectamente otro tipo de información que podría afectar en forma desproporcionada la privacidad de una persona, por lo cual debería efectuarse la publicación con los datos disociados tal como se establece en el art. 17 Literal D) de la Ley N° 18.331.

VII) Que en definitiva, es ajustado a derecho la publicación en la web en el marco de sus obligaciones de transparencia activa, siempre y cuando se consideren los parámetros antes señalados basados en la proporcionalidad, la finalidad y el equilibrio de los derechos en juego.

ATENCIÓN: 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 si bien no hay soluciones uniformes y globales, corresponde en general, la aplicación de los criterios señalados en los Considerandos I a VII.

2. Recomendar que esta consulta también sea derivada a la Unidad de Acceso a la Información Pública.

3.- Notifíquese, publíquese.

g.r.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 27, de 15 de noviembre de 2012.

Se dictamina sobre Proyecto de Ley presentado por los Señores Senadores Francisco Gallinal y Luis Alberto Lacalle (Carpeta 978/2012 de la Cámara de Senadores) para modificar la redacción del art. 22 de la Ley N° 18.331.

| DICTAMEN No. | | EXP. No. |
|--------------|------|-------------------|
| 27 | 2012 | 2012-2-10-0000879 |

Montevideo, 15 de noviembre de 2012.

VISTO: El Proyecto de Ley presentado por los Señores Senadores Francisco Gallinal y Luis Alberto Lacalle (Carpeta 978/2012 de la Cámara de Senadores) para modificar la redacción del art. 22 de la Ley N° 18.331.

RESULTANDO: I) Que el texto proyectado propone una serie de modificaciones al régimen de tratamiento de los datos personales comerciales, legislado actualmente en el citado art. 22 modificado por el art. 152 de la Ley N° 18.719.

II) Que las reformas propuestas refieren a la obligación de notificar a los deudores inscriptos en registros privados abiertos a la consulta por parte de terceros, a un procedimiento de descargos del titular del dato, a la disminución de los plazos de registro de los morosos, a la prohibición de registrar datos comerciales positivos y un régimen a seguir para el registro de morosidades provenientes de deudas ante organismos estatales.

CONSIDERANDO: I) Que el proyecto examinado se adecua en general al criterio tuitivo de la normativa sobre protección de datos personales.

II) Que con un criterio garantista, se comparte la solución de notificar a los deudores personas físicas su registro, con requisitos de plazo y contenido al efecto.

III) Que asimismo son de recibo las soluciones propuestas para el procedimiento impugnativo de descargos del titular del dato, con plazos resolutiveos y otras previsiones a cumplir por el registrador, así como la extensión del régimen sancionatorio contenido en el art. 35 de la Ley N° 18.331 a los registradores en caso de incumplimiento.

IV) Que respecto a otros contenidos del proyecto y sin perjuicio de lo antes indicado, este Consejo ha tenido oportunidad de pronunciarse anteriormente en el sentido de que “existen aspectos atinentes al funcionamiento del mercado económico, cuya consideración no compete, estrictamente, a esta Unidad” (Res. N° 1356, de 10-10-2010).

V) Que el proyecto de Ley examinado presenta algunos puntos susceptibles de adecuación, a saber extensión a las personas jurídicas del requisito de notificación registral y oportunidad de plantear descargos; remisión más genérica respecto del régimen sancionatorio del art. 2° (cita del art. 35 de la Ley N° 18.331, sus modificativos y concordantes) y empleo de los términos “acreedor o registrador” en vez de “obligado” en el inciso 2 de ese artículo.

ATENTO: A lo expuesto, y a lo establecido por los arts. 34 lits. F) y G) de la Ley N° 18.331, de 11 de agosto de 2008, y 23 lit. H) del Decreto N° 414/009 del Poder Ejecutivo, de 31 de agosto de 2009.

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

RESUELVE:

Hacer saber a la Cámara de Senadores y al Poder Ejecutivo el criterio de la Unidad Reguladora y de Control de Datos Personales sobre el Proyecto de Ley del los Sres. Senadores Francisco Gallinal y Luis Alberto Lacalle individualizado en el "Visto", remitiéndose copia del presente dictamen.

m.b.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 28, de 15 de noviembre de 2012.

Se dictamina sobre consulta formulada por la Intendencia de Paysandú respecto a eventual convenio de digitalización de documentos a suscribirse con otra entidad.

| DICTAMEN No. | | EXP. No. |
|--------------|------|-------------------|
| 28 | 2012 | 2012-2-10-0000743 |

Montevideo, 15 de noviembre de 2012.

VISTO: La consulta formulada por la Intendencia Municipal de Paysandú respecto de eventual convenio de digitalización de documentos a suscribir con la entidad Family Search International (FSI).

RESULTANDO: I) Que se solicita la opinión de la Unidad respecto de la adecuación del proyectado Acuerdo, del que se acompaña un modelo.

II) Que la fórmula proyectada contiene cláusulas que no se adecúan al derecho a la protección de datos personales vigente en nuestro país.

III) Que dicha inadecuación proviene fundamentalmente de lo consignado en la cláusula 6 que otorga a FSI la facultad de uso y tratamiento de las imágenes digitales para fines no lucrativos, y en la cláusula 10 donde se estipula el derecho de ambas partes a ceder los derechos del Acuerdo a sucesores y afiliados.

IV) Que asimismo se aprecian otras observaciones a tener presentes sobre las que bastaría introducir ciertos ajustes al modelo propuesto.

CONSIDERANDO: I) Que la comunicación de datos personales está regulada en el art. 17 de la Ley N° 18.331, siendo de regla la existencia de un interés legítimo en emisor y receptor, así como el previo consentimiento del titular de los datos.

II) Que las cláusulas 6 y 10 del Acuerdo proyectado no se compadecen con los preceptos legales en la materia, en especial el de recabar el previo consentimiento del titular de los datos, sin que quepa invocar ninguna de las excepciones que contempla la misma norma, resultando intrascendente la finalidad no lucrativa.

III) Que por tanto, para adaptarse a la ley, ambas cláusulas deben ser eliminadas en lo expresado, así como ajustar otros tramos del modelo en consideración, atendiendo a la necesidad de informar con mayor precisión las calidades de “responsable de la base de datos” y “encargado de tratamiento” respectivamente de ambos sujetos del Acuerdo, exigir a FSI la constitución de domicilio dentro del país a todos los efectos administrativos y procesales, y una prohibición de realizar el tratamiento fuera del país, caso en el cual se pasaría a un régimen de transferencia internacional de datos, con requisitos diferentes y más severos que los tenidos a la vista en este dictamen.

IV) Que complementando lo expuesto, surge que sería de buena técnica agregar al texto de la cláusula 8 una remisión expresa a la aplicación de la Ley N° 18.331, de 11 de Agosto de 2008, normas modificativas y reglamentarias.

ATENCIÓN: A lo precedentemente expuesto, lo dispuesto por los arts. 4° lit. D), 17 y 34 lit. F) de la Ley N° 18.331, de 11 de agosto de 2008, y el Informe Letrado N° 512/2012,

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

DICTAMINA:

Que el Acuerdo de Digitalización de Documentos de los Registros de Estado Civil sometido a la opinión de esta Unidad por la Intendencia de Paysandú, es conforme al derecho de la protección de datos personales salvo en aquellos aspectos señalados en los Considerandos de este Dictamen, los que deberán ser revisados para adecuarse al régimen vigente.

m.b.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 29, de 13 de diciembre de 2012.

Se dictamina acerca de si el Fondo de Solidaridad se encuentra habilitado para obtener cierta clase de datos personales que disponen los organismos tributarios recaudadores, para el mejor cumplimiento de sus cometidos.

| DICTAMEN No. | | EXP. No. |
|--------------|----|-------------------|
| 29 | 12 | 2012-2-10-0000755 |

Montevideo, 13 de diciembre de 2012.

VISTO: La consulta formulada por el Fondo de Solidaridad en cuanto a si se encuentra habilitado para obtener cierta clase de datos personales que disponen los organismos tributarios recaudadores, para el mejor cumplimiento de sus cometidos.

RESULTANDO: I) Que el órgano consultante es una persona de derecho público no estatal creada por la Ley N° 16.254 con el cometido de gestionar un sistema de becas de ayuda para la educación terciaria, mediante los fondos obtenidos de los organismos de recaudación tributaria en concepto de una contribución especial creada por la misma ley.

II) Que en orden al cumplimiento de estos cometidos, se alega no disponer de información actualizada acerca de los sujetos pasivos del tributo que administra, fundamentalmente por lo que hace al domicilio y otros datos de contacto.

III) Que la carencia anotada proviene de la circunstancia de que los registros que utiliza hasta este momento son los provenientes de la Universidad de la República, en su gran mayoría correspondientes a la época en que el profesional culminara sus estudios.

IV) Que ello ocasiona que el consultante no disponga de datos de contacto actualizados, que le permitan ejercitar sus cometidos legales con efectividad, vale decir promover el cumplimiento voluntario y sucedáneamente por medio de medidas administrativas y judiciales, de las obligaciones de los contribuyentes.

V) Que por el contrario, una información de este tenor actualizada es la que se encuentra en poder de la Caja de Jubilaciones y Pensiones de Profesionales Universitarios (CJPPU), la Caja Notarial de Seguridad Social (CNSS), la Dirección General Impositiva (DGI) y el Banco de Previsión Social (BPS).

CONSIDERANDO: I) Que el art. 6° del Decreto N° 325/002 en redacción dada por el art. 1° del Decreto N° 477/011, al reglamentar la Ley N° 16.254, precisa las facultades del órgano consultante para obtener la información que pretende.

II) Que el intercambio de información entre entidades públicas, estatales o no, está regulado por los arts. 157 a 160 de la Ley N° 18.719, entre cuyas obligaciones figura la de recabar el consentimiento de acuerdo con lo previsto en la Ley N° 18.331.

III) Que de su parte la comunicación de datos personales está regulada en el art. 17 de la Ley N° 18.331, y tiene como exigencias de regla o principio dos requisitos, a saber la existencia de un interés legítimo en emisor y receptor, y el previo consentimiento del titular de los datos.

IV) Que en el ocurrente, el interés legítimo en la comunicación aparece explicado y justificado, mientras que el requisito del consentimiento es abatible a través de algunas de las hipótesis que admite el régimen, y que para el caso son los “listados limitados” (art, 9° inc. 3° lit. C) de la Ley), y “el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal” (art. 9° inc. 3° lit. B) de la Ley).

V) Que aún cuando no se recabe el consentimiento de los titulares de los datos, procede de todos modos atenerse al cumplimiento de los restantes preceptos del régimen, en especial el respeto de la finalidad perseguida (contacto y facilitación para la adopción de medidas tendientes al cumplimiento voluntario o forzado de las obligaciones a cargo del contribuyente), limitación de la comunicación a aquellos datos estrictamente necesarios a esa finalidad, mantener la reserva y seguridad de los datos obtenidos, e inscribir la base de datos en el Registro que lleva la Unidad.

ATENCIÓN: A lo precedentemente expuesto, lo dispuesto por la normativa citada en el cuerpo, el art. 34 lit. F de la Ley N° 18.331 de 11 de agosto de 2008, y el Informe Letrado N° 515/2012, El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

DICTAMINA:

Que el Fondo de Solidaridad está habilitado para requerir la comunicación de datos personales de los sujetos pasivos del tributo que administra, a los organismos y con el alcance planteado en los Considerandos del presente Dictamen.

m.b.

Fdo.: Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 30, de 13 de diciembre de 2012.

Se dictamina respecto a la consulta formulada por la Auditoría Interna de la Nación (AIN) sobre el régimen a aplicar a cierta información que recibe proveniente de la Dirección General Impositiva (DGI).

| DICTAMEN No. | | EXP. No. |
|--------------|----|-------------------|
| 30 | 12 | 2012-2-10-0000669 |

Montevideo, 13 de diciembre de 2012.

VISTO: La consulta formulada por la Auditoría Interna de la Nación (A.I.N.) respecto al régimen a aplicar a cierta información que recibe proveniente de la Dirección General Impositiva (D.G.I.).

RESULTANDO: I) Que atento a lo expresado por la consultante, se trata de información relativa a estados contables de firmas contribuyentes, que la A.I.N. recibe de la D.G.I. para el cumplimiento de sus cometidos y amparada en el secreto tributario, todo ello conforme al art. 503 de la Ley N° 18.362.

II) Que para facilitar consultas la A.I.N. vuelca la referida información proveniente de D.G.I. en una base de datos.

III) Que específicamente se consulta: A) si corresponde que la A.I.N. registre esta base de datos ante la Unidad. B) Si en caso de recibir una petición de acceso del titular de los datos, se debe incluir como parte de la respuesta la información comunicada por la D.G.I.

CONSIDERANDO: I) Que la base de datos objeto de consulta ingresa en el art. 24 de la Ley N° 18.331, que dispone que “la creación modificación o supresión de bases de datos pertenecientes a organismos públicos deberán registrarse...”.

II) Que no es de aplicación ninguna de las excepciones al ámbito objetivo de la ley, consignadas en el art. 3° de la Ley, ni tampoco las hipótesis reguladas en los arts. 25 y 26 de la misma.

III) Que el secreto tributario no es motivo fundado para negarle acceso al interesado, a la información que el mismo ha generado y entregado a un organismo público.

IV) Que en caso que la titular de los estados contables sea una persona jurídica, tampoco es óbice para negarle el acceso a esta información, desde el momento que las personas jurídicas son titulares del derecho a la protección de sus datos personales “en cuanto corresponda” (art. 2° de la Ley).

ATENTO: A lo precedentemente expuesto, lo dispuesto por los arts. 3°, 14, 24 y 34 lit. F) de la Ley N° 18.331, de 11 de agosto de 2008, así como el Informe Letrado N° 510/2012,

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

DICTAMINA:

1. Que la base de datos personales objeto de consulta, que contiene información sobre estados contables de firmas contribuyentes entregada a la Auditoría General de la Nación por la Dirección General Impositiva, debe ser registrada ante la Unidad por la primera de las nombradas, en calidad de responsable de la misma.

2. Que no es obstáculo legal para el ejercicio del derecho de acceso de parte del titular de los datos (persona física o jurídica indistintamente), el secreto tributario prescripto en el art. 503 de la Ley N° 18.362, debiendo en tal caso limitarse el acceso a los mencionados estados contables, originariamente entregados a la D.G.I. por sus titulares, y comunicados a la A.I.N por disposición legal, sin otro tipo de informaciones.

m.b.

Fdo.: Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen N° 31, de 20 de diciembre de 2012.

Se dictamina acerca de la consulta formulada respecto a la legalidad de la comunicación de las imágenes almacenadas en videocámara a solicitud de terceros.

| DICTAMEN No. | | EXP. No. |
|--------------|----|-------------------|
| 31 | 12 | 2012-2-10-0000855 |

Montevideo, 20 de diciembre de 2012.

VISTO: La consulta formulada en cuanto a la legalidad de la comunicación de las imágenes almacenadas en videocámara, a solicitud de terceros.

RESULTANDO: I) Que un cliente habría olvidado su aparato telefónico celular en el mostrador de la consultante, y existen elementos de sospecha de que el mismo podría habérselo apropiado otra persona que se hubiera aproximado luego al mismo mostrador.

II) Que la consultante dispone de videocámara en el lugar, ubicado dentro de un shopping center, en la que podrían haber quedado registradas las imágenes correspondientes a este insuceso.

III) Que el personal de seguridad del shopping center le ha solicitado a la consultante la comunicación de dichas imágenes, lo que motiva la presente consulta.

CONSIDERANDO: I) Que las imágenes de personas constituyen datos personales a los que se aplica el régimen jurídico de protección de datos personales según lo ha editado ya la Unidad a través de su Dictamen N° 10 de 16-04-2010.

II) Que sin perjuicio de otros, existen en la materia dos principios o reglas esenciales, que son el de reserva y el de consentimiento.

III) Que en virtud de la aplicación y juego armónico de ambos principios, la respuesta a la consulta formulada será negativa ya que no se observa que existan en el caso ninguna de las condiciones o hipótesis legales en las que procede comunicar datos personales a terceros, por parte de quien dispone de ellos.

IV) Que en casos como el ocuriente, corresponde que el propio responsable de la base de datos de videovigilancia, a través de personal autorizado, verifique si se cumplen las sospechas existentes, y en su caso de trámite a la intervención policial y judicial correspondientes.

V) Que en cuanto al personal de seguridad del shopping center se le puede brindar un informe objetivo de lo que arroje la visualización de las imágenes, siempre que no permita identificar ni hacer identificable al presunto autor del delito, labor que -como ya se expresara- es de cargo de las autoridades competentes.

VI) Que toda base de datos pública o privada debe inscribirse en el Registro habilitado al efecto por la Unidad, deber que el consultante no ha cumplido y deberá hacerlo.

ATENTO: A lo precedentemente expuesto, lo dispuesto por los arts. 4º lit. D, 9º inc. 3º lit. B), 17 inc. 3º lit. B), 29 y 34 lit. A) de la Ley Nº 18.331, de 11 de agosto de 2008, el Dictamen Nº 10, de 16-04-2010 y el Informe Letrado Nº 508/2012,

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

DICTAMINA:

1. Ratificar lo resuelto en este órgano por Dictamen Nº 10, de 16 de abril de 2010, en cuanto a que las imágenes almacenadas en videocámaras colocadas en lugares de uso público, constituyen una especie de datos personales abarcada, como tal, por la Ley Nº 18.331 y sus normas complementarias.
2. En consecuencia, salvo consentimiento del titular, o ejercicio de funciones propias de los poderes del Estado, u obligación legal, u orden de la justicia competente, no procede revelar dichas imágenes ni comunicarlas a terceros.
3. Intímese a AA Uruguay S.R.L. el registro de su base de datos personales de videovigilancia y toda otra de la que sea responsable, en el plazo de treinta (30) días, y bajo apercibimiento.

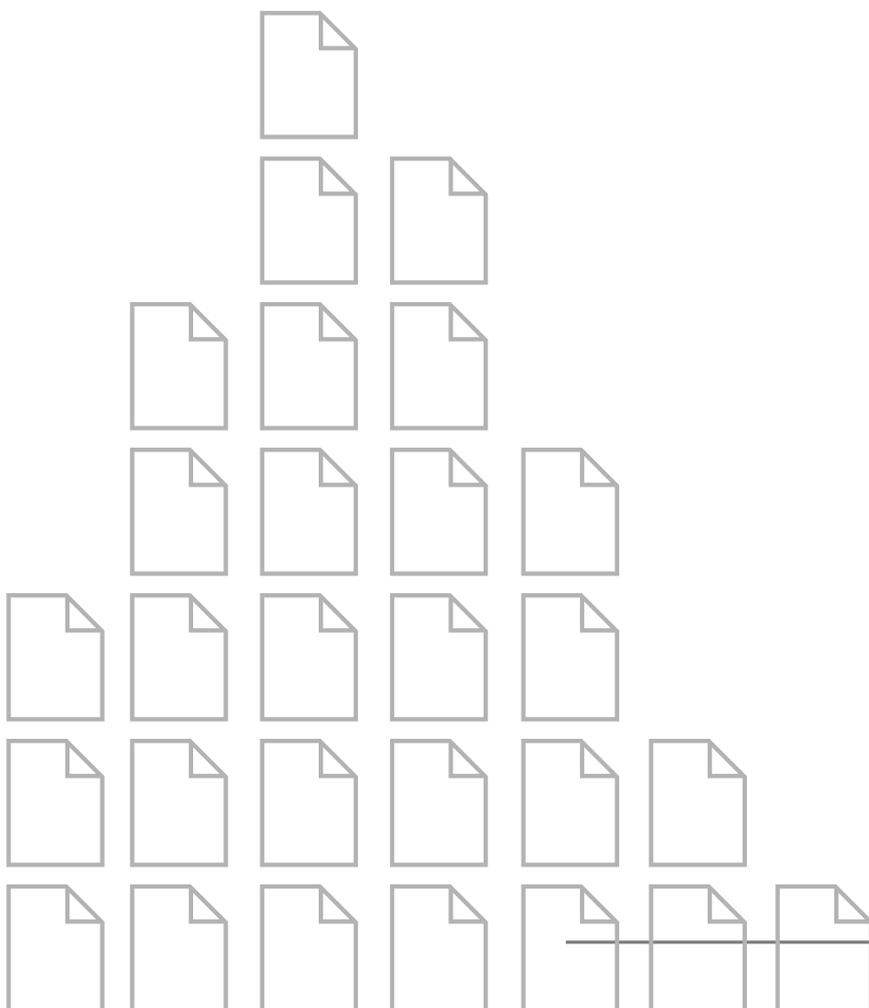
m.b.

Fdo.: Dr. Felipe Rotondo

Consejo Ejecutivo URCDP



Informes



Informe N° 5, de 3 de enero de 2012.

Se informa en relación a la consulta de si resulta procedente la aplicación de la Ley 18.331 a los objetivos del grupo “Apostasía Colectiva en Uruguay”

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 5 | 12 | 2011-2-10-0001074 |

Montevideo, 3 de enero de 2012.

Ref. Consulta sobre Apostasía y Habeas Data

-I- Antecedentes

El Sr. AA, en virtud de haber conformado un grupo llamado “BB”, solicita asesoramiento a la Unidad Reguladora y de Control de Datos Personales, acerca de si resulta procedente en la especie, la aplicación de la Ley N° 18.331.

-II- Análisis

1. Apostasía - Definición.-

Según el Diccionario de la Real Academia Española¹ apostatar significa: “Negar la fe de Jesucristo recibida en el bautismo; Dicho de un religioso: Abandonar irregularmente la orden o instituto a que pertenece; Dicho de un clérigo: Prescindir habitualmente de su condición de tal, por incumplimiento de las obligaciones propias de su estado”.

2. Aplicación de la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data (LPDP).-

2.1. Base de Datos.-

Conforme la definición que brinda la LPDP en su artículo 4° literal A), se considera base de datos al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Los datos contenidos en los libros de bautismo en tanto asientan nombres, apellidos y hecho del bautismo, constituyen datos personales, de acuerdo con la definición prevista en el artículo 4° literal D) de la LOPD: “información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables”.

Ahora bien ¿puede afirmarse que ese conjunto de datos que conforman los libros de bautismo, es organizado y estructurado al amparo de las disposiciones normativas citadas?

Sobre este punto, la Agencia Española de Protección de Datos y la jurisprudencia de la Audiencia Nacional se afiliaron al criterio de considerar a los libros bautismales, como ficheros. El Tribunal Supremo Español, por el contrario, a partir de una sentencia de 19 de septiembre de 2008, ha entendido que “son una pura acumulación de datos que comporta una difícil

¹ http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=apostatar Página visitada el 2 de enero de 2012.

búsqueda, acceso e identificación en cuanto no están ordenados ni alfabéticamente, ni por fecha de nacimiento, sino sólo por las fechas de bautismo”.

Coincidiendo con tal postura, la organización o estructura a que se hace referencia en la definición de base de datos aludida ut supra no está presente en los libros bautismales, en tanto no hay un orden preestablecido donde los datos personales del bautizado puedan encontrarse fácilmente, sin esfuerzos desproporcionados.

Se trata de libros donde se registra el hecho histórico del bautismo celebrado, por fecha de realización. Veamos que ni siquiera reviste importancia la fecha del nacimiento. Basta ejemplificar lo dificultoso y arduo que puede ser encontrar el asiento del bautismo cuando en la mayoría de los casos ya no solo no se cuenta con la fecha aproximada, sino siquiera con el año en que la celebración fue verificada, comportando al decir del Tribunal Supremo, una difícil búsqueda, acceso e identificación.

2.2. Derecho de supresión o eliminación.-

La supresión o eliminación solo procede cuando se verifiquen perjuicios a los derechos e intereses legítimos de terceros; notorio error, o contravención a lo establecido por una obligación legal (artículo 15 LPDP).

El artículo 13 del Decreto 414/009 prevé que la utilización de los datos personales por terceros, resulte ilegítima, o que resulten ser inadecuados o excesivos.

Ninguna de estas hipótesis se constata en la especie.

Por otra parte, el artículo 13 citado, añade que la supresión no procederá cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas.

2.3. Derecho de rectificación y actualización.-

Tampoco pueden ejercitarse los derechos de rectificación o actualización, en tanto no puede afirmarse que la información contenida en los Libros de Bautismo sea inexacta o incompleta. (artículo 10 y 11 Decreto 414/009).

En consonancia con esto, debemos abordar uno de los principios que consagra la LPDP, cual es el principio de veracidad, que se balancea precisamente con dos características fundamentales, la exactitud y la actualidad.

Según el diccionario de la Real Academia Española, el significado de veraz es que dice, usa o profesa siempre la verdad; y el de actualidad, tiempo presente.

El artículo 7º prevé que “...cuando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados”.

En razón de lo expuesto, en los Libros de Bautismo no cabe apreciar ninguna inexactitud de datos, en cuanto en los mismos se recoge un dato histórico cierto, cual es el referente al bautismo de una persona.

-III- Conclusiones

1. Atendiendo a la normativa de protección de datos, los Libros bautismales no configuran strictu sensu la categoría de bases de datos, sino simplemente un conglomerado de datos que

implica dificultad de búsqueda, acceso e identificación.

En efecto, al no estar organizados o estructurados ni alfabéticamente ni por fecha de nacimiento, sino precisamente por la fecha de celebración del bautismo, es *conditio sine qua non* el previo conocimiento de la parroquia y la fecha precisa donde se formalizó, circunstancia que refuerza la idea de inaccesibilidad para terceras personas que no podrían solicitar partidas de bautismo que no los involucren.

2. De la mano con lo anterior, debemos recordar que el asiento del bautizo no es un dato que pueda tildarse de inexacto total o parcialmente, erróneo o falso como exige la normativa analizada para apostatar, o en los términos de la LPDP, dar mérito a una supresión, rectificación o actualización como la pretendida en autos.

En el bautizo, se registra un hecho histórico de que se celebró uno de los sacramentos que otorga la Iglesia Católica, sin apostillas.

Es todo cuanto tengo que informar.

Fdo. Dra. M^a José Rodríguez Tadeo
Derechos Ciudadanos

Informe N° 11, de 5 de enero de 2012.

Se informa sobre denuncia contra institución bancaria por realizar reiteradas llamadas al celular sin consentimiento.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 11 | 12 | 2011-2-10-0000699 |

Montevideo, 5 de enero de 2012

Ref. Denuncia AA contra institución bancaria

-I- Antecedentes

El 19 de octubre de 2011 AA presenta denuncia online contra BB por entender que éste ha vulnerado la Ley de Protección de Datos Personales, al llamarla a su celular en reiteradas oportunidades sin su consentimiento, con el propósito de ofrecerle determinados productos. La URCDP para un mejor pronunciamiento, procede a dar traslado de la denuncia a la empresa quien toma vista el 1° de diciembre de 2011 pero no presenta descargos.

Una vez vencido los plazos correspondientes, se realiza informe jurídico de acuerdo con la legislación vigente en la materia.

-II.- Análisis de la denuncia presentada

La Sra. AA aduce que recibe llamadas en su celular por parte del Banco BB pero nunca autorizó que realizaran esas llamadas para ofrecerle créditos y seguros. Agrega que, por más que ha pedido que no la llamen más a ese celular que es para trabajar, siguen y siguen llamando.

La denuncia refiere a un hecho alcanzado por las disposiciones vigentes en materia de protección de datos personales. En este sentido, el artículo 4 literal d) de la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (en adelante LPDP) define al dato personal como “información de cualquier tipo referido a personas físicas o jurídicas determinadas o determinables”.

En razón de ello, el número de celular es un dato personal cuyo tratamiento debe ser analizado a la luz de la ley antes mencionada y su reglamentación:

1. 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”.

2. El art. 9° Literal C) establece que “El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse”. Agrega que: “No será necesario el previo consentimiento cuando: C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento”. Como vemos el celular es un dato personal que no integra este elenco.

3. Por su parte, el art. 21 de la Ley establece que: “En la recopilación de domicilios, reparto de documentos, publicidad, venta u otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento (subrayado nuestro).

En el caso que se analiza y según las afirmaciones de la denunciante, el número de celular no ha sido proporcionado por ella a la institución bancaria. Tampoco surge del expediente que dicho número figure en documentos accesibles al público, o que de alguna forma se haya recabado el consentimiento de la titular. Hay que tener presente que BB no ha presentado descargos a efectos de dilucidar el tema.

Por lo expuesto, cabe concluir que estamos ante un tratamiento de datos personales que vulnera la Ley N° 18.331 (arts. 4°, 9° y 21).

-IV- Sobre la inscripción de la Base de Datos de BB

La Ley establece que para que una base de datos se considere legítima es necesario que se encuentre inscrita ante el registro que el órgano de control lleva a estos efectos (Principio de Legalidad, Art. 5 de la Ley). Asimismo, establece la obligación de que todos los organismos públicos, empresas y personas físicas inscriban sus bases de datos (art. 28 y 29 de la LPDP). Consultado el sistema informático de la URCDP creado a tales efectos, surge que BB ha iniciado el proceso de inscripción de sus bases de datos tal como lo indica la Ley.

-V- Sobre la potestad sancionatoria de la URCDP

El Consejo Ejecutivo de la URCDP tiene potestades sancionatorias ante el incumplimiento de la Ley, pudiendo imponer sanciones que van desde la observación y el apercibimiento, hasta multa de hasta quinientas mil unidades indexadas y clausura de las bases de datos por un plazo de hasta seis días hábiles (artículo 35 de la LPDP en su redacción actual dada por la Ley N° 18.719, de 27 de diciembre de 2010, de Presupuesto Nacional del período 2010-2014). Este procedimiento se encuentra regulado en el artículo 31 del Decreto N° 414/009. Asimismo, el régimen sancionatorio encuadra dentro de la discrecionalidad que posee la Administración teniendo en consideración los principios de razonabilidad y proporcionalidad. Atento a ello, será el Consejo Ejecutivo de la URCDP quien podrá determinar la sanción de acuerdo con la normativa vigente.

Corresponde recordar que BB ya ha sido sancionado con apercibimiento, según surge de la Resolución N° 720/2011, de 14 abril de 2011, recaída en el Expediente N° 3030/2010. Tal extremo debería ser tenido en cuenta por el Consejo Ejecutivo de la URCDP a los efectos de graduar la sanción a imponer.

Atendiendo a la posibilidad de que recaiga sanción en el expediente, se debería dar nuevamente vista previa al denunciado en los términos de los arts. 75 del Decreto N° 500/991, de 27 de setiembre de 1991.

Fdo. Dra. Graciela Romero
Derechos Ciudadanos

Informe N° 27, de 19 de enero de 2012.

Se informa sobre consulta acerca de la instalación de una cámara de videovigilancia en la cocina-comedor de un particular.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 27 | 12 | 2011-2-10-0000818 |

Montevideo, 19 de enero de 2012.

Ref. Consulta AA acerca instalación de cámara de video vigilancia

-I- Introducción

Según la consulta presentada se desea recibir información acerca de las eventuales consecuencias jurídicas que tendría contratar el servicio de video vigilancia ofrecido por ANTEL (<http://www.antel.com.uy/antel/personas-yhogares/movil/servicios/con-costo/Video-vigilancia>), dado que la intención es instalar la cámara en la cocina-comedor del domicilio particular, donde durante el día laboral está trabajando la niñera, contratada para el cuidado de los hijos menores de edad.

El siguiente análisis, -según lo solicitado por la Dra. María José Viega-, se realizará a la luz del derecho de los trabajadores a la privacidad y a protección de sus datos personales en el ámbito laboral, así como el deber de cuidado y protección que poseen los padres respecto a sus hijos menores de edad, contracara del derecho de éstos a ser protegidos y a crecer en un ambiente seguro.

-II- Análisis de los principales aspectos de la consulta

A) Sobre el sistema de video vigilancia ofrecido por ANTEL

El anuncio de ANTEL indica que por primera vez en Uruguay habrá un sistema de vigilancia y seguridad para el hogar, la oficina, el comercio o donde se requiera. A través del mismo se podrá monitorear en tiempo real desde el PC, laptop o a través del celular.

El consultante entonces pretende contratar el servicio para monitorear el ámbito de su hogar, concretamente la cocina comedor del mismo. En este caso, corresponde considerar que estamos en un ámbito doméstico, que no sería tal para la persona que desempeña funciones cuidando a los hijos menores de edad de quien consulta.

B) Sobre datos Personales en el ámbito laboral, derecho a proteger la seguridad del hogar y de los hijos menores de edad.

La evolución que se ha producido en materia de derecho a la intimidad y a la privacidad, ha llevado a que el “derecho a estar solo”, adquiera una dimensión más social y colectiva, llegándose así a la madurez del derecho a tener el control de nuestros datos personales y a que los mismos sean protegidos.

Coincidiendo con lo que expresan algunos autores, “la intimidad como una disciplina jurídica ha perdido su carácter exclusivo individual y privado, para asumir progresivamente una significación pública y colectiva, consecuencia del cauce tecnológico. Esto es, en palabras de Lusky, la privacy, más que un mero sentido estático de defensa de la vida privada del

conocimiento ajeno, tiene la función dinámica de controlar la circulación de informaciones relevantes para cada sujeto. Por su parte, Fried se pronuncia en el mismo sentido, señalando que la privacy no implica sencillamente la falta de información sobre nosotros por parte de los demás, sino más bien el control que tenemos sobre las informaciones que nos conciernen”.² Además “Pérez Luño, entre otras cosas, señala que la propia noción de intimidad o privacidad es una categoría cultural, social e histórica. Por lo que ahora este concepto ha pasado de una concepción cerrada y estática de la intimidad a otra abierta y dinámica. Puesto que ahora se contempla la posibilidad de conocer, acceder y controlar las informaciones concernientes a cada persona”³.

Por ende cuando tenemos que analizar un caso como el que se nos plantea, donde se entrecruzan varios derechos (derecho del consultante a proteger la seguridad de su hogar y la seguridad de sus hijos, así como el derecho a la intimidad y a la protección de datos personales de la trabajadora doméstica), creemos conveniente enmarcar dicho análisis en esta evolución. Ya no podemos hablar del “derecho a estar solo” en el sentido estricto de estas palabras, sino de cómo podemos ejercer el derecho a controlar la información que los demás obtienen sobre nosotros.

El consultante tiene derecho a garantizar la seguridad de su hogar, en este caso mediante la utilización de un dispositivo tecnológico, que pone a su disposición ANTEL. En este sentido, el art. 7° de nuestra Constitución establece que, “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 establecieron por razones de interés general”.

Por su parte, el art. 10 establece que “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. Ningún habitante de la República será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe”, y el art. 11 reconoce a su vez que el hogar de cada persona es un sagrado inviolable.

También tiene, no sólo el derecho, sino la obligación de proteger a sus hijos menores de edad. El art. 41 de la Constitución señala que “el cuidado y educación de los hijos para que éstos alcancen su plena capacidad corporal, intelectual y social, es un deber y un derecho de los padres.” Por otra parte, el art. 3° del Código de la Niñez y la Adolescencia establece que “todo niño y adolescente tiene derecho a las medidas especiales de protección que su condición de sujeto en desarrollo exige por parte de su familia, de la sociedad y del Estado”.

En definitiva, como se expresa en el Dictamen N° 10/010 de la Unidad Reguladora y de Control de Datos Personales (URCDP), de 16 de abril de 2010, la videovigilancia 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”.

2 Aristeo GARCÍA GONZÁLEZ. *La Protección de datos Personales. Derecho Fundamental del Siglo XXI. Un Estudio Comparado*. <http://www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm>. Página consultada 27/04/2010

3 Aristeo GARCÍA GONZÁLEZ. *La Protección de datos Personales. Derecho Fundamental del Siglo XXI. Un Estudio Comparado*. <http://www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm>. Página consultada 27/04/2010

En este caso, como ya se ha expresado, creemos que existe por parte del consultante un interés legítimo, así como otros derechos que deben ser sopesados y valorados.

C) Sobre el derecho a la PDP de la trabajadora

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, entre los principios generales se señala que el tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuaníme y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación de empleo del trabajador.⁴

Ello es así porque, como muy bien lo expresa el Informe del G29, “los trabajadores no dejan su derecho a la vida privada y a la protección de datos cada mañana a la puerta de su lugar de trabajo. Esperan legítimamente encontrar allí un grado de privacidad, (...). Este derecho debe, no obstante, conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con cierta eficacia la empresa, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los trabajadores. Estos derechos e intereses constituyen motivos legítimos que pueden justificar la adopción de medidas adecuadas destinadas a limitar el derecho a la vida privada de los trabajadores”.⁵ En nuestro país, los tribunales han entendido que, más allá de la debida protección de la intimidad y la dignidad de los trabajadores, hay un margen de control al que tienen derecho los empleadores. Por ejemplo en la Sentencia del Juzgado Letrado de Trabajo de 1º Turno N° 4 de 7 de marzo de 2006⁶, 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 (...)”

Por otra parte, la Ley establece en su art. 3º que se aplicará a los datos personales registrados en cualquier soporte, pero señala que no será de aplicación a las bases de datos mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Al respecto, corresponde analizar cómo considerar el ámbito donde se va a videovigilar desde la óptica del trabajador, porque no hay que olvidar que además de ser el hogar del consultante, es el ámbito laboral del personal doméstico.

⁴ *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.

⁵ *GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS - ARTÍCULO 29 - 5401/01/ES/ Final. WP 55. Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo. Aprobado el 29 de mayo de 2002.*

⁶ *Sentencia del Juzgado Letrado de Trabajo de 1º Turno N° 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>

Justamente la Guía de Videovigilancia de la AGPD formula esa pregunta: “¿Se entiende por uso particular y/o doméstico la instalación de una cámara por una persona en su domicilio para vigilar las tareas de quien realiza tareas de limpieza o cuidado de niños?”. Ellos enmarcan la respuesta analizando la normativa laboral que rige para España y establecen que “el artículo 20.3 del Estatuto de los Trabajadores (E.T.) habilita al empleador al tratamiento de las imágenes de sus trabajadores (...) pero es imprescindible que, al menos, los trabajadores sean informados al respecto. Por tanto, en principio, siempre que estos trabajadores sean informados se pueden instalar cámaras para controlar su actividad dentro del domicilio. No hay que olvidar que siempre habrá que tener en cuenta la proporcionalidad entre la finalidad y el tratamiento”.

Por otra parte la Guía de INTECO sobre Videovigilancia y PDP⁷, en su sección “Seguridad en el hogar”, establece que “las imágenes captadas por videocámaras instaladas en el entorno doméstico con fines de seguridad, al considerarse éstas las realizadas por una persona en el marco de una actividad puramente privada o familiar quedan excluidas de los tratamiento de la LOPD y de la Instrucción 1/2006, siempre y cuando no afecte al personal que presta servicios en el interior del domicilio”. En tanto en la sección “Control laboral en entornos domésticos”, establece que “es legítima la utilización de cámaras en entornos domésticos para el control laboral de personas ajenas contratadas, por ejemplo para el desempeño de tareas de mantenimiento, cuidado de niños o cualquier otro servicio prestado en el interior del domicilio”.

Por otra lado, la Ley N° 47/2005⁸ de Nueva Gales del Sur, que regula la videovigilancia en el ámbito laboral, establece en su art. 10 que debe existir un previo aviso que debe darse por lo menos 14 días antes de que comience a vigilarse. Si la vigilancia de los empleados ya ha comenzado, cuando un empleado es contratado por primera vez, debe avisársele al ser contratado, de lo contrario, deberá darse comienzo a la vigilancia, por lo menos de 14 días, después de que ya ha sido contratado.

En tanto, en el art. 15 se establece que un empleador no puede realizar vigilancia de un empleado en el vestuario, inodoro, ducha, baño o instalaciones similares de los lugares de trabajo, y en el art. 16 se prohíbe la vigilancia mientras que el empleado no esté trabajando, o no esté en su lugar de trabajo.

-III- Conclusión

En definitiva, partiendo de la base de que la imagen es un dato personal sin dudas su tratamiento debe estar sujeto a la normativa de protección de datos personales. Aún así, en el caso analizado no sería necesario obtener el consentimiento de la persona afectada por el sistema de videovigilancia. En este sentido, el art. 9° de la Ley N° 18.331 establece que el tratamiento de los datos es lícito cuando el titular hubiera prestado su consentimiento libre, previo, expreso e informado, salvo las excepciones que establece la norma.

⁷ Instituto Nacional de Tecnologías de la Comunicación (INTECO). Guía sobre videovigilancia y protección de datos personales. Edición: Junio 2011

⁸ Ley N° 47 de 2005. Nueva Gales del Sur. http://www.austlii.edu.au/au/legis/nsw/consol_act/wsa2005245/ Página vista 7/12/2011

Entre esas excepciones, en el Numeral D), se establece que si esos datos derivan de una relación contractual por ejemplo, y son necesarios para su desarrollo o cumplimiento no se exige recabar dicho consentimiento en forma expresa. Esto sería cuando ese tratamiento es necesario para el adecuado desenvolvimiento de la relación laboral de los trabajadores de una empresa, o como en el caso, de una relación laboral referida al cuidado de los niños.

En este sentido se pronuncia la Guía de la INTECO ya antes mencionada, respecto a que no se requiere recabar el consentimiento “si existe una relación jurídica que así lo establece y la captación es necesaria para su mantenimiento o cumplimiento, si la grabación forma parte de las funciones de la Administración pública o persigue el interés vital de los individuos grabados”.

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 se deberá:

a) Informar expresamente al trabajador, pues de esta forma la videovigilancia 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 videovigilado (art. 13 de la Ley N° 18.331).

c) Utilizar esos datos sólo para la finalidad para la cual son recabados, esto quiere decir que los datos que se obtienen no podrán ser utilizados para fines distintos (art. 8° de la Ley N° 18.331). Complementando este punto, y de acuerdo a lo expresado en el Informe Técnico de la Ing. Viviana García respecto a que, “este tipo de memorias permite el respaldo histórico en otros dispositivos de mayor capacidad tales como discos duros, CD, DVD, etc.” cabe recordar que los datos 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.

d) Respetar los espacios privados del trabajador, como baños, dormitorios o vestuarios, pues la videovigilancia en estos casos afecta su 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° núm. 2 de la Ley N° 18.331).

e) 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, pues considerando nuevamente lo expresado en el Informe Técnico de la Ing. Viviana García, el servicio permite el monitoreo de hasta 20 usuarios, sujeto a la previa autorización del Administrador.

Fdo. Dra. Graciela Romero

Derechos Ciudadanos

Informe N° 64, de 8 de febrero de 2012.

Se informa sobre cláusula de confidencialidad a incorporar en el marco del Fondo Concursable LA 21

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 64 | 12 | 2012-2-10-0000097 |

Montevideo, 8 de febrero de 2012.

Ref. Consulta sobre cláusula de confidencialidad a incorporar en el marco del Fondo Concursable LA 21

-I- Antecedentes

Se solicita a esta Unidad la redacción de una cláusula de confidencialidad a ser incorporada en el Fondo Concursable LA 21 correspondiente a “Servicios de desarrollo de software y migración de datos para el sistema “Vía Trabajo” de la Dirección Nacional de Empleo, utilizado por el INEFOP”, que se encuentra en ejecución.

Aducen que en el marco del referido proyecto, el proveedor necesita llevar una copia de la base de datos a su oficina para trabajar en la migración de los datos y que dicho extremo no acarrea inconvenientes en tanto ello está acordado con el jefe del Centro de Cómputos del Ministerio.

-II- Análisis

1. La situación que plantea el consultante no implica una comunicación de datos en el sentido que le otorga la Ley N° 18.331, sino que estamos ante una tarea llevada a cabo por un “encargado de tratamiento”.

La Ley define “encargado de tratamiento” como la persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento. (artículo 4º, literal H)).

En mérito a ello, resulta aplicable lo dispuesto por el artículo 14, inciso 2º del Decreto reglamentario N° 414/009, en cuanto establece:

“No se considera comunicación o cesión de datos el acceso por parte de un encargado de tratamiento, que resulte necesario para la prestación de un servicio al responsable, salvo que este acceso implique la existencia de un nuevo vínculo entre el encargado del tratamiento y el titular.”

2. Ello no obsta que en razón de la tarea desarrollada, se deba dar cumplimiento con los principios consagrados en la Ley N° 18.331, esencialmente los de finalidad, reserva, seguridad y responsabilidad (artículos 8º, 10, 11 y 12 Ley N° 18.331, artículos 7º y 8º, Decreto N° 414/009).

-III- Conclusión

1. En virtud de lo expuesto, se sugiere la siguiente cláusula para incorporar al contrato con el proveedor del servicio:

Obligación de confidencialidad

En la tarea de migración que desarrolle el firmante respecto de la base de datos deberá cumplir con las siguientes obligaciones:

a. Mantener absoluta confidencialidad y reserva de toda la información que se maneje y de todo conocimiento que se tenga sobre ella.

b. Utilizar la información únicamente para la finalidad establecida, quedando prohibido al firmante todo uso o reproducción para su beneficio propio o de terceros, así como toda comunicación no autorizada.

c. Adoptar medidas de seguridad que sean idóneas para garantizar la integridad, confidencialidad y disponibilidad de la información.

d. Informar al (responsable) de cualquier vulneración de seguridad que se pueda verificar en cualquier fase del tratamiento de la información.

2. La presente cláusula podrá ser aplicable en las tareas de migración que se desarrollen, siempre y cuando éstas no posean características disímiles o particularizadas a la presente, que ameriten un nuevo análisis por parte del Órgano de Control.

Es todo cuanto tengo que informar.

Fdo. Dra. M^a José Rodríguez Tadeo

Derechos Ciudadanos

Informe N° 78, de 8 de febrero de 2012.

Se informa sobre denuncia presentada contra empresa consultora por envío de correo electrónico no deseado.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 78 | 12 | 2011-2-10-0000586 |

Montevideo, 8 de febrero de 2012.

Ref. Denuncia AA contra BB Consultores.

I. ANTECEDENTES

I.A. Con fecha 13 de Setiembre de 2011, AA presentó ante la Unidad Reguladora y de Control de Datos Personales una denuncia contra la empresa BB Consultores en virtud de haber recibido por parte de ésta, correos electrónicos no deseados (Spam).

I.B. Solicita se inicien las actuaciones administrativas correspondientes en virtud de las cuales se procede a dar vista de la denuncia a la empresa BB Consultores a través de telegrama colacionado. Con fecha 11 de Octubre de 2011, se presenta a tomar vista a CC, presidente de la empresa.

I.C. El día 24 de Octubre de 2011 la empresa BB presenta sus descargos en tiempo y forma, procediéndose a dar vista de éstos al denunciante. Este último toma vista de las actuaciones con fecha 21 de Noviembre de 2011 y presenta sus descargos con fecha 5 de Enero del corriente, pasado el plazo legal para hacerlo.

Presenta documentación que acredita que se encontraba fuera del país (copias de pasaporte), por períodos intermitentes de tiempo, lo cual no acredita que no le ha sido posible evacuar la vista en tiempo y forma.

Recibidos los descargos se pasa el expediente a análisis técnico y posteriormente a la presente informante.

II. ANÁLISIS DE LA DENUNCIA

II.A. Hechos. El denunciante afirma que la empresa BB Consultores le envía correos electrónicos no deseados o spam a su casilla de correo electrónico xx@gmail.com, cuyas copias acompaña a su denuncia. Alega que nunca había entrado en contacto con la empresa y que desconoce cómo han accedido a su correo electrónico. Por otra parte indica que procedió a enviar correos a la denunciada solicitando ser removido de su lista.

Por su parte, la empresa BB Consultores, según anexos que presenta, alega que la suscripción a su red es absolutamente voluntaria y que la realiza cada interesado pudiendo incluso ser realizada por cualquier persona. Por otra parte, indica que el tratamiento que se da a los datos es confidencial y que existe en cada correo enviado, la posibilidad de darse de baja de la red, en forma explícita al pie de éste. Respecto a los intentos de darse de baja realizados por AA, indica que la casilla de correo a la cual fueron enviados no cuenta con la posibilidad de enviar una respuesta, tratándose únicamente de una casilla de envíos.

II.B. Marco legal del Spam en Uruguay. En nuestro país no contamos actualmente con normativa específica en materia de spam o correo electrónico no deseado. Por otra parte, de acuerdo a la normativa en materia de protección de datos personales dada por la Ley N° 18.331, de 11 de agosto de 2008, el correo electrónico constituye un dato personal. Conforme con lo dispuesto en el artículo 21 de la Ley 18.331 cuando la empresa quiera realizar publicidad, el correo electrónico debe obtenerse en alguna de las hipótesis previstas por la norma, ya sea que se haya obtenido de documentos accesibles al público, haya sido facilitado por su titular u obtenido con su consentimiento.

II.C. Consentimiento de AA. De los descargos formulados por la empresa BB Consultores no resulta probado que el denunciante hubiese consentido el tratamiento de su correo electrónico a fin de recibir ofertas de empleo por parte de la denunciada. La empresa denunciada afirma que no contaba con las medidas necesarias para cumplir con las disposiciones legales en materia de consentimiento previstas en la Ley N° 18.331, a la luz de las cuales para el tratamiento de datos personales, entre ellos el correo electrónico, es necesario contar con el consentimiento del titular de los datos. Además exige que sea prestado en forma libre, previa, expresa, documentada e informando al titular de la finalidad para la cual se recaban sus datos.

III. CONCLUSIONES

III.A. La denuncia se origina en el tratamiento del dato personal correo electrónico correspondiente a AA por parte de la empresa BB Consultores. No se probó en las presentes actuaciones que el denunciante hubiese consentido el tratamiento de su correo electrónico a fin de recibir ofertas de trabajo por parte de la denunciada. En virtud de ello, dicho tratamiento no resulta adecuado a la Ley N° 18.331, dado que no se ha contado con el previo consentimiento del titular del dato personal.

III.B. De acuerdo a lo expuesto y a la primariedad de los ilícitos cometidos y de acuerdo a lo preceptuado en los artículos 9° y 35 de la Ley N° 18.331 (en su redacción dada por el artículo 152 de la Ley N° 18.719 de 27 de Diciembre de 2010), se recomienda la aplicación de una sanción de observación a la empresa BB Consultores.

III.C. Por otra parte, se recomienda que se tengan presentes las sugerencias técnicas realizadas por la Ing. Viviana García con respecto a los sistemas de suscripción y baja, así como a las buenas prácticas para la lucha contra el spam.

Es todo cuanto tengo que informar.

Fdo. Dra. Jimena Hernández

Derechos Ciudadanos

Informe N° 106, de 27 de febrero de 2012.

Se informa en relación a la consulta sobre utilización de Identificadores de Objetos - OIDs para identificar usuarios.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 106 | 12 | 2012-2-10-0000148 |

Montevideo, 27 de febrero de 2012.

Ref. Consulta AA acerca instalación de cámara de video vigilancia

-I- Antecedentes

La consulta presentada a la URCDP el 14 de febrero de 2012 refiere a la utilización de OIDs para identificar el ingreso de un usuario a la red (logueo), con el fin de dar respuesta a las inquietudes formuladas por funcionarios del Ministerio de Relaciones Exteriores que consideran que se debería requerir el previo consentimiento de los usuarios.

Para un mejor pronunciamiento de la Unidad se solicita a A/S Mauro Ríos la elaboración de un informe desde el punto de vista técnico.

-II- Análisis desde el punto vista de la PDP

La consulta contiene dos puntos centrales a ser analizados:

- a) Sobre la utilización de OIDs para identificar personas.

Respecto a este punto cabe tener presente la definición y alcance de los identificadores únicos. Al respecto la Unidad Nacional de Asignación de OIDs (UNAOID), entiende como Objeto a todo tangible e intangible, y los OIDs pueden identificar a cualquiera de esos objetos, pero mayormente a los utilizados por las Tecnologías de la Información y la Comunicación (TIC), como por ejemplo países, instituciones, oficinas, dispositivos tecnológicos, firmas digitales, servicios, documentos, etc.

La importancia y alcance de estos identificadores está dada porque al ser utilizados correctamente, se constituyen en la base de la interoperabilidad en los sistemas de información de la Administración Pública, con el resto de los sectores sociales y con el resto de los países del mundo, así como también permite tener la capacidad de trazabilidad e inventario de todos los bienes y servicios del Estado.

Por otra parte, el A/S Mauro Ríos en su informe expresa que, en cuanto a la identificación de personas en Uruguay se “corresponde a la Cédula de Identidad emitida por la Dirección Nacional de Identificación Civil. Para un ciudadano de otro país corresponde a su documento de identificación aceptado por la Dirección Nacional de Migración. En los documentos que posean letras las mismas son sustituidas por número de dos posiciones, asignando a la letra A el 00, a la B el 01 y así sucesivamente”.

En definitiva, el identificador se utiliza con el número de Cédula de Identidad de la persona y el Código correspondiente al país, y se aplica tanto a ciudadanos uruguayos como a turistas, etc. (en este caso con número de pasaporte).

Agrega Mauro Ríos en su informe que el “uso de un “OID de persona”, bajo las especificaciones técnicas de la UNAOID, para autenticarse ante un sistema informático, cumple la misma función que la definición de un usuario de dichos sistemas, utilizando cualquier nomenclatura, ya sea el nombre de la persona, un usuario fantasía o incluso su Cédula de Identidad”.

Por ende, “el uso de OID como identificación de usuarios, no aporta información per se respecto al usuario en sí más allá de su Cédula de Identidad. Ni siquiera su nombre está asociado en primera instancia si no se implementa un sistema de, por ejemplo “fichas” u objetos en el sistema informático, donde se asocie determinada Cédula de Identidad al resto de la información de cada usuario, algo que no está implícito en la identificación de esos usuarios con un OID de persona”.

B) Sobre la eventual obligación de solicitar el consentimiento de los usuarios de acuerdo al art. 9° de la Ley.

El art. 9° Literal C) establece que “El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse”, pero agrega que: “No será necesario el previo consentimiento cuando: C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento”.

En el caso en cuestión, la utilización del número de Cédula de Identidad o Pasaporte, así como el código del país que indica la nacionalidad, no exige recabar el previo consentimiento del titular para ser tratados.

Por otra parte, respecto a la posibilidad de identificar a los usuarios en un sistema (logueo), -ya sean funcionarios o interesados en trámites, etc., también puede aplicar el art. 9° B) que indica que no se requiere el previo consentimiento cuando los datos se recaben para el ejercicio de las funciones propias de los poderes del Estado (en este caso del Ministerio) o en virtud de una obligación legal. A su vez, un organismo público está obligado a controlar el ingreso de usuarios a la red, sobre todo por cuestiones vinculadas a la seguridad de la información

En caso de que la consulta refiera específicamente a los empleados o funcionarios como usuarios de la red, cabe tener presente que existe una relación contractual, profesional o laboral entre los mismos y el Ministerio, que lleva implícita la posibilidad de éste de controlar si ingresan o no a la red (Art. 9° D), también por cuestiones vinculadas a la seguridad de la información. Ese control se puede realizar identificando al usuario con su nombre, un OID o un usuario fantasía tal como indica en su informe técnico Mauro Ríos.

Cabe tener presente además, que en nuestro país, los tribunales han entendido que, más allá de la debida protección de la privacidad de los trabajadores, hay un margen de control al que tienen derecho los empleadores. Por ejemplo en la Sentencia del Juzgado Letrado de Trabajo de 1º Turno N° 4 de 7 de marzo de 2006⁹, se expresa que “la propia naturaleza de la relación subordinada da lugar a que la eficacia de estos derechos pueda verse limitada”.

Justamente por ello se establece entre las excepciones del art. 9, en el Numeral D), que si esos datos derivan de una relación contractual por ejemplo, y son necesarios para su desarrollo o cumplimiento no se exige recabar dicho consentimiento en forma expresa, ya que ese tratamiento es necesario para el adecuado desenvolvimiento de la relación laboral de los trabajadores de una empresa o de un organismo público.

Fdo. Dra. Graciela Romero

Derechos Ciudadanos

⁹ *Sentencia del Juzgado Letrado de Trabajo de 1º Turno N° 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>

Informe N° 153, de 19 de marzo de 2012.

Se informa sobre consulta del Centro Integral del Personal de ANTEL (CIPA) sobre la obligación de inscribir las bases de datos.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 153 | 12 | 2012-2-10-0000229 |

Montevideo, 19 de marzo de 2012.

Ref. CONSULTA CIPA SOBRE REGISTRO DE BASE DE DATOS

-I- Antecedentes

Se consulta si es obligatorio o no registrar la base de datos de afiliados de uno de los sindicatos de ANTEL.

Se manifiestan dudas sobre tal obligatoriedad por cuanto parte de los datos que integran la base provienen de un tercero, concretamente del servidor ADINET propiedad de ANTEL, el que posee su “política de privacidad” a través de un enlace Internet que no funciona.

-II- Análisis

La respuesta a la consulta formulada es concluyente, en el sentido de que la circunstancia alegada por la consultante no tiene relación ni influencia alguna respecto de la obligación de registro a su cargo.

Para la ley, quienes deben inscribir son los responsables “de la base de datos o del tratamiento”. Y se entenderá por tales no solamente a los “propietarios de la base de datos” sino también a quien “decida sobre la finalidad, contenido y uso del tratamiento” (art. 4° lit. K, 28 y 29 de la Ley N° 18.331).

Es evidente que el sindicato cumple los requisitos que se acaban de relevar, por varios motivos: porque las direcciones de correos electrónicos no son la única especie de dato personal que integra su base de datos según la misma consulta ilustra; porque de todos modos es la consultante, y no otra persona, la que decide sobre finalidad, contenido y uso de tales especies de datos, a partir de su libreta de direcciones.

La situación no es diferente a la inmensa mayoría de responsables de bases de datos que, si bien integran parte de la base con datos en formato electrónico provenientes de servidores ajenos a su titularidad, de todos modos hacen un tratamiento propio de esos datos, condición suficiente para que, quienes lo hacen, adquieran la calidad de responsables de la base de datos o tratamiento de éstos.

Sin perjuicio de lo expresado, y dado que la consultante pone en conocimiento un asunto de competencia de la Unidad como es la falta de funcionamiento del enlace **<http://www.privacidad.adinet.com.uy>**, hecho comprobado por el suscrito, se sugiere tomar medidas instructivas al respecto.

-III- En conclusión

La consultante tiene obligación legal de inscribir su base de datos de afiliados a través del sistema de registro en línea dispuesto para ello en el sitio web de la Unidad **www.datospersonales.gub.uy**

Con relación a la falta de funcionamiento del enlace de Internet **http://www.privacidad.adinet.com.uy**, se sugiere instruir vista por expediente aparte a abrirse a tales efectos.

Fdo. Dr. Marcelo Bauzá

Derechos Ciudadanos

Informe N° 201, de 19 de abril de 2012.

Se informa sobre consulta realizada por la Agencia Nacional de Vivienda (ANV) sobre pertenencia y uso del correo electrónico entregado a los usuarios, así como de la regulación de la privacidad de la información contenida en los mismos.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 201 | 12 | 2012-2-10-0000296 |

Montevideo, 19 de abril de 2012.

Ref. Consulta sobre naturaleza y control del correo electrónico entregado a los usuarios.

I- Introducción

La consulta proviene de la Agencia Nacional de Vivienda y refiere a la pertenencia y al uso del correo electrónico entregado a los usuarios, así como a la regulación de la privacidad de la información contenida en los mismos.

Por tratarse de una consulta realizada por el integrante del Comité de Seguridad de la Información de un organismo público, se considerará que los términos “empresa” y “usuarios” refieren a organismo o administración y a empleados o funcionarios en el sentido amplio, respectivamente.

El siguiente análisis se realizará a la luz del derecho de los trabajadores a la privacidad y a protección de sus datos personales en el ámbito laboral, así como de la potestad de control y de discrecionalidad que posee la administración pública en el ámbito de sus funciones, con relación a las actividades desarrolladas por sus funcionarios, así como de sus recursos.

-II- Sobre el correo electrónico institucional como herramienta de trabajo

Respecto a la pertenencia del correo otorgado al trabajador o funcionario, ya sea por una empresa o por un organismo público, es clara la jurisprudencia laboral en cuanto a considerar que es una herramienta y un recurso propio del empleador, entregado en tal carácter al trabajador para que cumpla con las tareas asignadas.

Así ha quedado plasmado en varios fallos de la justicia laboral. Por ejemplo en la Sentencia N° 312 del Tribunal de Apelaciones en lo Laboral de 1° Turno, de 26 de agosto de 2004¹⁰, “el Tribunal revoca la sentencia del Juzgado Letrado de Trabajo de 10° Turno N° 90, de 29 de agosto de 2003, con relación al correo electrónico laboral expresa que su naturaleza propone una nueva interpretación en la medida que se considera que el trabajador no es el dueño de su cuenta sino que lo es el empresario que proporciona la misma para fines absolutamente laborales, y por tanto las normas deben tender a proteger los intereses de una persona jurídica como propietaria de la cuenta de correo, que la asigna a un trabajador para su uso y administración en nombre del cargo que desempeña y para fines estrictamente laborales”.

¹⁰ Ver en Base de Datos Jurisprudencia Informática. Instituto Derecho Informático de Facultad de Derecho de la UDELAR y AGESIC. <http://www.jurisprudenciainformatica.gub.uy/jurisprudencia/ficha.jsp?id=49>

En tanto, en la Sentencia N° 91¹¹ del Juzgado Letrado de Primera Instancia de Trabajo de 9° Turno, de 4 de diciembre de 2006, “se desestima la indemnización por despido pues resulta configurada la mala conducta del trabajador por el uso del correo electrónico para fines personales, en horario laboral. La Empresa, dio sendos avisos a todo el personal –vía correo electrónico- invitando a que el uso de dichos medios técnicos se aplicara en forma exclusiva a actividades laborales, para mejorar la performance de los equipos, todo ello en el marco de un uso adecuado de los poderes de dirección del empleador y la consecuente potestad disciplinaria. El Tribunal entendió que no interesa el tenor de las conversaciones vía mail mantenidas, sino el hecho mismo de haberlas mantenido durante el horario laboral, a pesar de claras advertencias en contrario de la empleadora, (...) el trabajador hizo un uso claramente indebido del correo electrónico, bien material de la empresa, destinado al cumplimiento de sus fines”.

Reafirmando lo ya expresado, en la Sentencia N° 39¹² del Juzgado Letrado de Primera Instancia de Trabajo de 16° Turno, de 16 de diciembre de 2008, se resuelve respecto al control de la casilla de correo del trabajador como violación de la privacidad y el uso abusivo de las herramientas de la empresa por parte del trabajador. En este caso, “afirma el Juez que la jurisprudencia se ha pronunciado entendiendo que configura notoria mala conducta, pues el envío de mensajes particulares a través de correo electrónico utilizando el actor los medios informáticos del empleador en horario de trabajo constituye un hecho que debe ser comprendido, sin esfuerzo, en la eximente legal de notoria mala conducta”.

Por último, ya específicamente en el ámbito administrativo, el Tribunal de lo Contencioso Administrativo en la Sentencia N° 205¹³, de 12 de junio de 2008, confirma “la resolución por la cual la Corte Electoral sancionó al actor con suspensión sin goce de sueldo, anotación en el legajo personal, transformando su separación provisional del Centro de Cómputos, en definitiva”, debido a que “surge probado (...) que el actor creó en forma violatoria de los deberes funcionales, una dirección de correo electrónico dentro del sistema informático de la Administración demandada. A través de dicha cuenta, intercambiaba mensajes entre funcionarios de diversas reparticiones de la Corte Electoral, tanto de Montevideo como de ciudades del interior, correspondencia que tenía fundamentalmente contenido gremial y político”.

En definitiva en cuanto a la pertenencia del correo electrónico entregado a los usuarios, cabe concluir que es un recurso que pertenece al organismo u empresa que lo provee, por lo cual a su vez, se poseen ciertas potestades de control y de supervisión que habilitan a adoptar las medidas necesarias y proporcionales tendientes a salvaguardar la seguridad del sistema y el desarrollo adecuado de las actividades laborales.

11 Ver: <http://www.jurisprudenciainformatica.gub.uy/jurisprudencia/ficha.jsp?id=146>

12 Ver: <http://www.jurisprudenciainformatica.gub.uy/jurisprudencia/ficha.jsp?id=162>

13 Ver: <http://www.jurisprudenciainformatica.gub.uy/jurisprudencia/ficha.jsp?id=24>

-IV-Sobre la regulación de la privacidad de la información contenida en los mismos
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, entre los principios generales 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”¹⁴.

Agrega el mismo documento que: “En todas las reglamentaciones internacionales y nacionales que restringen el uso de datos personales (...) se reconoce como indispensable la vigilancia continua de los trabajadores (...) para cumplir la finalidad por la cual se establece la vigilancia, es decir, el correcto funcionamiento del sistema. Por tanto, no deben servir para controlar o vigilar el comportamiento y los desplazamientos de los trabajadores”.

Como muy bien lo expresa el Informe del G29¹⁵, “los trabajadores no dejan su derecho a la vida privada y a la protección de datos cada mañana a la puerta de su lugar de trabajo, (...) no obstante sus derechos deben conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con cierta eficacia la empresa, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los trabajadores. Estos derechos e intereses constituyen motivos legítimos que pueden justificar la adopción de medidas adecuadas destinadas a limitar el derecho a la vida privada de los trabajadores”.

Agrega el mencionado informe que “el principio de proporcionalidad excluye por lo tanto el control general de los mensajes electrónicos y de la utilización de Internet de todo el personal, salvo si resulta necesario para garantizar la seguridad del sistema (...). Si es posible, el control del correo electrónico debería limitarse a los datos sobre tráfico de los participantes y a la hora de una comunicación más que al contenido, si ello es suficiente para satisfacer las necesidades del empleador. Si el acceso al contenido de los mensajes es indispensable, convendría tener en cuenta el respeto de la vida privada de los destinatarios externos e internos de la organización”.

Considera por su parte este grupo de expertos, que “La tecnología ofrece al empleador importantes posibilidades de evaluar la utilización del correo electrónico por sus trabajadores, comprobando, por ejemplo, el número de mensajes enviados y recibidos o el formato de los documentos adjuntos; por ello la apertura efectiva de los mensajes electrónicos es desproporcionada”.

¹⁴ *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*

¹⁵ *GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS - ARTÍCULO 29 - 5401/01/ES/Final. WP 55. Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo. Aprobado el 29 de mayo de 2002.*

De todas maneras, refiriéndonos exclusivamente a la regulación de la privacidad de la información contenida en los correos electrónicos institucionales o sea al texto y encabezado de los correos enviados de la cuenta entregada al usuario, -y considerando especialmente lo expresado por la jurisprudencia de nuestro país-, los mismos no deberían contener información personal del trabajador en sentido estricto. En este caso, es el trabajador quien tiene la carga de usar esa cuenta de correo sólo para desempeñar las tareas inherentes a su cargo.

No obstante ello, muchas veces habrá información, -contenida en los correos electrónicos institucionales-, que está directamente relacionada con el trabajo pero que refiere a la privacidad del trabajador o a datos sensibles que requieren legalmente una protección especial. Por ejemplo, es lógico que a través de este correo se comuniquen al empleador los problemas de salud que impiden que el trabajador se presente a trabajar, determinados datos médicos, incluso datos que pueden relevar origen racial o étnico o la actividad sindical que se lleva a cabo por parte de los trabajadores, etc.

Debido a esto, cada responsable de base de datos o de tratamiento de datos, está obligado a adoptar medidas de seguridad para proteger adecuadamente los datos personales que posee. Esas medidas deben ser adecuadas para garantizar que los datos permanezcan seguros y confidenciales, evitando que sean modificados, consultados o tratados por terceros que no están autorizados para ello, y que por cualquier medio sean divulgados sin autorización (arts. 10, 11, 12, 18 y 19 de la Ley N° 18.331).

En este sentido, el G29¹⁶ “llama la atención sobre el papel del administrador del sistema, un trabajador cuyas responsabilidades en materia de protección de datos son importantes. Es fundamental que el administrador del sistema, así como cualquier persona que tenga acceso a datos personales de los trabajadores durante las operaciones de control, esté sometido a una obligación estricta de secreto profesional respecto a la información confidencial a la que pueda acceder”.

-V- Conclusiones

1. Tanto la administración pública como las empresas, tienen derecho a controlar las cuentas de correo electrónico de su titularidad, entregadas a los funcionarios u empleados para el desempeño de sus funciones, limitándose en lo posible a los datos sobre tráfico más que al contenido en sí de las comunicaciones, salvo que ello sea necesario.

2. No obstante, en consonancia no sólo con la Ley de Protección de Datos Personales, sino con principios que inspiran el derecho a una legítima defensa, al debido proceso y a relaciones laborales enmarcadas en la buena fe, es necesario informar expresamente y por anticipado al trabajador (art. 13 de la Ley N° 18.331).

¹⁶ GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS - ARTÍCULO 29 - 5401/01/ES/Final. WP 55. Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo. Aprobado el 29 de mayo de 2002.

En el Documento “Repertorio de recomendaciones prácticas de la OIT”, también se señala que “Los trabajadores y sus representantes deberían ser informados de toda actividad de acopio de datos, de las reglas que la gobiernan y de sus derechos¹⁷. Sólo excepcionalmente cabe el monitoreo reservado ya que según el repertorio de la OIT ya citado “El empleador está autorizado al uso de la vigilancia secreta únicamente cuando existan sospechas razonablemente justificadas de actividades delictivas u otras infracciones graves. Como ejemplo de infracción grave, se menciona el acoso sexual, que puede no ser calificado necesariamente como actividad delictiva”.

3. La forma en que debe informarse debe ser expresa, precisa e inequívoca acerca del mecanismo que se utilizará, la finalidad que tiene y el alcance del mismo. Es conveniente que se haga mediante una circular o reglamento de circulación interna con un mecanismo idóneo que permita dejar constancia de que cada funcionario ha sido notificado (art. 13 de la Ley N° 18.331). Constatado el abuso, el trabajador también deberá ser informado, salvo razones imperiosas que justifiquen continuar con la vigilancia encubierta, cuando ésta proceda.

4. Es responsabilidad del funcionario utilizar la cuenta de correo institucional sólo para las tareas relacionadas con su trabajo, aunque hay determinada información que, -aunque relacionada al desempeño de su actividad-, revelará datos de su vida privada, incluso datos sensibles. Cabe tener presente que el documento de la OIT ya citado, en este sentido indica que, “Los empleadores, los trabajadores y sus representantes deberían cooperar en la protección de los datos personales y en la elaboración de una política de empresa que respete la vida privada de los trabajadores”.

5. Es obligación del organismo u empresa utilizar esa información sólo para la finalidad para la cual ha sido recabada, esto quiere decir que los datos que se obtienen no podrán ser utilizados para fines distintos a los informados (art. 8° de la Ley N° 18.331), así como se deberá garantizar la seguridad y confidencialidad de los mismos.

Fdo. Dra. Graciela Romero

Derechos Ciudadanos

¹⁷ *Repertorio de recomendaciones prácticas de la OIT adoptado en Ginebra del 1° 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*

Informe N° 209, de 24 de abril de 2012.

Se informa sobre consulta presentada por Ministerio de Transporte y Obras Públicas (MTO), sobre uso de datos personales en desarrollo informático.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 209 | 12 | 2012-2-10-0000295 |

Montevideo, 24 de abril de 2012.

Ref. Consulta MTO sobre uso de datos personales en desarrollo informático

-I- Antecedentes

Se consulta sobre la adecuación de un nuevo sistema informático (en etapa de desarrollo) para la gestión de puertos, a la normativa vigente sobre protección de datos personales. El mencionado sistema será administrado por la Dirección Nacional de Hidrografía dependiente del Ministerio de Transporte y Obras Públicas.

-II- Análisis

Dado que su creación está en fase de desarrollo, y la consulta se formula en términos amplios sin precisar qué tratamientos específicos de datos personales realiza el sistema proyectado, se expondrá en términos sintéticos y prácticos lo que debe hacer la Dirección de Hidrografía en la materia.

La consultante podrá obtener mayor asesoramiento que el derivado del presente Informe, a través de entrevistas y charlas que puede solicitar y acordar con la Unidad.

La protección de datos personales es un derecho fundamental de rango constitucional, con su reconocimiento y marco regulatorio vigente en el país a través del art. 72 de la Constitución de la República, la Ley N° 18.331, de 11 de agosto de 2008, su modificativa Ley N° 18.719, de 27 de diciembre de 2010, y sus decretos reglamentarios N° 414/009, de 31 de agosto de 2009 y N° 664/008, de 22 de diciembre de 2008.

Los titulares de este derecho son las personas físicas y jurídicas (estas últimas “en cuanto corresponda” como lo expresa el art. 2° de la ley), y el cumplimiento del derecho se asegura o garantiza a través de una serie de principios generales y obligaciones, que deben cumplir los responsables de las bases de datos personales o tratamientos de los mismos.

Los deberes básicos a cumplir, son los siguientes:

1 – Registrar la base de datos a través de la página web de la URCDP, para lo cual existen instructivos y formularios accesibles en el sitio web de la Unidad **www.datospersonales.gub.uy**

2 - Recolectar y utilizar el mínimo necesario de datos personales, de modo conforme la finalidad y destino de la base de datos o tratamiento a realizar (arts. 7° y 8° de la Ley).

3 – Recoger el consentimiento libre, previo, expreso e informado del titular del dato,

salvo que se trate de datos que no requieran de dicho consentimiento (art. 9° de la ley).

4 – Mantener los datos veraces y actualizados (art. 7° de la Ley), y eliminarlos una vez que su uso ha dejado de ser necesario o pertinente (art. 8° de la Ley).

5 – Adoptar las medidas de seguridad y confidencialidad necesarias (art. 10 y 11 de la Ley).

6 – Responder por toda violación de las disposiciones de la ley.

7 – Si se van a comunicar los datos a terceros, hacerlo bajo los requisitos que marca la ley (art. 17 y 23 de la Ley).

8 – No realizar tratamientos de “datos sensibles” salvo hipótesis de excepción y bajo requisitos especiales (art. 18 de la Ley).

9 – Instaurar procedimientos ágiles y sencillos que permitan al titular del dato ejercitar una serie de derechos: información, acceso, rectificación, actualización, inclusión, supresión e impugnación de valoraciones personales (arts. 14 a 16 de la Ley)

-III- Conclusión

Se sugiere tener por evacuada la consulta en los términos genéricos precedentes, sin perjuicio de hacer saber al consultante que dispone de otras posibilidades de asesoramiento y asistencia que brinda la Unidad (art. 34 lit. A) de la Ley). En tal sentido, en el sitio web **www.datospersonales.gub.uy** podrá encontrar amplia documentación ilustrativa del régimen a cumplir, además del formulario en línea para proceder al registro de la base de datos personales a crear. También podrá ampliar su consulta inicial hacia aspectos más concretos, así como petitionar entrevistas y charlas informativas al personal involucrado.

Fdo. Dr. Marcelo Bauzá

Derechos Ciudadanos

Informe N° 213, de 25 de abril de 2012.

Se informa sobre consulta Intendencia de Rocha sobre comunicación de datos personales de beneficiarios de una casa de refugio.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 213 | 12 | 2012-2-10-0000326 |

Montevideo, 25 de abril de 2012.

Ref. Consulta Intendencia de Rocha

-I- Antecedentes

La consulta ha sido realizada por la Intendencia Departamental de Rocha y refiere a la entrega de determinada información solicitada por un edil de la Junta Departamental de Rocha, con relación al funcionamiento de la Casa Refugio “Comuna de Rocha” que atiende a personas en situación de calle.

En dicho pedido de informes, se solicita proporcionar información sobre la cantidad de personas que han ocupado el refugio desde el mes de octubre de 2011 a la fecha, así como el nombre completo de los ocupantes y su lugar de origen.

La Intendencia, frente a la posibilidad de informar la identidad de los beneficiarios del refugio manifiesta sus dudas en tanto, en el caso se contraponen el derecho que tiene el edil a solicitar determinada información, con el derecho a la protección de datos personales de esas personas, que además se encuentran en una especial situación de vulnerabilidad social.

-II-Análisis de los datos solicitados

Con respecto a la cantidad y origen de los ocupantes, al tratarse sólo de datos disociados que refieren a la cantidad de personas existentes en un determinado período de tiempo así como al lugar de donde provienen, no cabría realizar objeciones jurídicas.

En cambio, al analizar la posibilidad de proporcionar los nombres de cada uno de los ocupantes, corresponde realizar las siguientes consideraciones:

1.- Derecho a la Protección de Datos como derecho humano

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, por lo que está comprendido en el art. 72 de la Constitución Nacional.

Nuestra Constitución a su vez, también contiene otras normas que garantizan derechos relacionados, como el derecho al honor¹⁸ y a la privacidad¹⁹.

Por ello, si bien es cierto que el pedido de informes realizado por el Edil Departamental se

¹⁸ Artículo 7°. 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.

¹⁹ 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 establecieron por razones de interés general.

enmarca en lo establecido en el art. 284 de la Constitución, corresponde tener presente también, que la Ley N° 18.331 consagra un derecho humano y un sistema de protección especial que emana de la propia Carta Magna, así como del Derecho Internacional de los Derechos Humanos²⁰.

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

Ello es así, porque a la hora de admitir o no la entrega de determinada información de particulares, que por determinado motivo se encuentra en poder de un organismo público; indefectiblemente debe existir un juicio de proporcionalidad basado en la idoneidad, la necesidad y el equilibrio de los derechos en juego. Esto significa a su vez, 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.

2.- Juicio de proporcionalidad y principio de finalidad

En el caso de marras, corresponde analizar qué tipo de datos podrían ser adecuados y no excesivos con relación a la finalidad implícita en el pedido de informes realizado por el edil, que no podría ser otra que la de controlar la gestión y el correcto funcionamiento del refugio. De acuerdo con ello, la Ley N° 18.331 recoge una serie de principios que delimitan las responsabilidades de quienes poseen y/o realizan tratamiento de datos personales y, que además, 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).

Entre esos principios se encuentra el de finalidad (art. 8°), verdadero pilar de la protección de datos personales, que establece que los datos objeto de tratamiento no podrán utilizarse para finalidades distintas o incompatibles a aquéllas que motivaron su obtención.

A su vez, el art. 7° de la Ley contempla la necesidad de que el tratamiento y/o comunicación de un determinado dato personal, deba ser proporcional a la finalidad que lo motiva.

En el caso, coincidiendo con lo expresado por la Intendencia, la comunicación de los nombres de los beneficiarios, no sólo vulneraría la protección de datos personales y la privacidad, sino la propia dignidad de estas personas.

Cabe recordar por otra parte, que el Consejo Ejecutivo de la URCDP ya se ha expresado en tal sentido en el Dictamen N° 15, de 15 de setiembre de 2011, ante la consulta presentada por

²⁰ *La Declaración Universal de Derechos Humanos de 10 de diciembre de 1948 establece en su Artículo 12 que “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”. También el Pacto de Derechos Civiles y Políticos de 16 de Diciembre de 1966, en el Artículo 17 recoge este derecho con una redacción similar a la anterior. La Convención Americana sobre Derechos Humanos en el Artículo 11 establece que: “Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Nadie puede ser objeto de injerencias abusivas o arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o esos ataques”.*

el Fondo de Solidaridad, acerca de si debía o no informar la identidad de los beneficiarios de las becas que otorga la Institución.

En esa oportunidad, 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”.

Dicha conclusión aplica perfectamente al caso, por lo que no correspondería entonces develar la identidad de las personas que han utilizado los servicios brindados por la Casa Refugio “Comuna de Rocha”.

-III- Conclusiones

Cabe concluir que, desde el punto de vista de la protección de datos personales, la Intendencia de Rocha estaría sólo legitimada para entregar al solicitante, información relacionada con el lugar de origen y la cantidad de personas que han utilizado el refugio en el período comprendido entre el mes de octubre de 2011 hasta la fecha.

En cambio, respecto a la identidad de cada una de estas personas, debe considerarse que no corresponde legalmente brindar dicha información, ya que vulnera el derecho a la protección de datos y no se ajusta a los principios de proporcionalidad y de finalidad, verdaderos pilares de la Ley N° 18.331.

Fdo. Dra. Graciela Romero
Derechos Ciudadanos

Informe N° 265, de 14 de mayo de 2012.

Se informa sobre consulta acerca del sistema de intercambio de datos de defunciones en sistema digital que actualmente se está implantando en el Ministerio de Salud Pública.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 265 | 12 | 2012-2-10-0000404 |

Montevideo, 21 de mayo de 2012.

Ref. Consulta intercambio datos de defunción sistema MSP

-I- Introducción

La consulta refiere al sistema de defunciones digital que actualmente está implantando el Ministerio de Salud Pública (MSP). Esto habilita a que los médicos certifiquen la defunción de una persona a partir del ingreso al sistema informático con su firma, al igual que lo hacen para el certificado de nacido vivo.

Se indica que actualmente existe un web service que provee información de las defunciones certificadas por el MSP, al que sólo accede el Registro Civil, sin embargo otros organismos o entidades, como por ejemplo el BROU, también han planteado el interés de acceder al mismo. Si bien el MSP no tiene inconvenientes en habilitar el acceso, se plantean las siguientes dudas:

1- ¿Cuál es la restricción en materia de protección de datos personales?.

2- ¿Qué validez legal tiene el certificado electrónico del MSP sin la intervención del Registro Civil, organismo que se ocupa de emitir las partidas correspondientes?.

3- ¿Cómo debe ser el esquema de funcionamiento de los organismos que requieren acceder a esta información, por ejemplo para dar por finalizado un beneficio social, etc.?

4- ¿Debe formalizarse el acuerdo entre Registro de Estado Civil y MSP para acceder a información del último de los mencionados? ¿Cómo se debe hacer?.

-II- Sobre restricciones que atañen a la PDP: consentimiento, finalidad y reserva

De acuerdo a 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, se deben adoptar todas aquellas medidas necesarias para promover el intercambio de información pública o privada, pero en este último caso con autorización del titular (o su representante) cuando así se requiera, conforme la Ley N° 18.331.

En este sentido, el art. 158 de la referida norma establece que, a los efectos del intercambio de información entre Entidades Públicas, estatales o no, una de las obligaciones consiste en recabar el consentimiento, de acuerdo con lo previsto en la Ley N° 18.331, cuando el objeto de intercambio refiere a información privada o de particulares que requiere el previo consentimiento informado.

Además, en el art. 159 se establece que las Entidades Públicas deberán ajustar su actuación a una serie de principios, entre ellos algunos que inspiran especialmente la protección de datos

personales como el de previo consentimiento informado, el de finalidad y el de confidencialidad y seguridad, los cuales a su vez, sirven de criterio interpretativo para resolver las cuestiones que puedan suscitarse.

Es importante tener presente que aún respecto a aquellos datos que no requieren previo consentimiento informado, también las Entidades Públicas deberán observar los principios que estructuran la Ley N° 18.331. En este sentido, esto es lo expresado en los comentarios realizados por el Grupo del Artículo 29 (G29), en la consulta realizada en el marco del proceso de adecuación de Uruguay a la Unión Europea.

No obstante ello, un aspecto central a considerar en el marco de la consulta presentada, es la finalidad del intercambio que deberá estar en consonancia con lo establecido en la Ley N° 18.331.

En este sentido debe analizarse el marco de poderes y competencias que han sido asignadas legalmente a cada organismo, para determinar si es posible aplicar algunas de las excepciones establecidas en la Ley antes mencionada.

Al respecto, el art. 9° B) de la misma, establece que no será necesario el previo consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, y además el art. 17 indica que los datos personales 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° ya mencionado.

Cabe apuntar entonces, que atento a los cometidos asignados al MSP en la Ley de su creación N° 9.202, de 12 de enero de 1934, y normas posteriores, así como al Registro Civil, por las Leyes N° 13.737 (art. 154) y N° 14.269, y demás normas existentes, no sería exigible recabar el consentimiento informado de los titulares de los datos.

Ello se debe a que resulta aplicable el inciso B) del artículo 9° de la Ley N° 18.331, que exime de tal requisito cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

La excepción de recabar el previo consentimiento informado rige asimismo, para la comunicación de datos que desarrolle el Organismo en el ámbito de sus cometidos. No obstante, en el caso de que dicha comunicación se realice a otras entidades, como por ejemplo el BROU, se deberá recabar el previo consentimiento porque los cometidos específicos de esta entidad no habilitan a interoperar directamente con el MSP, sino que corresponde que los datos sobre las defunciones de sus clientes, se los proporcione directamente al Registro de Estado Civil.

En cuanto a la reserva y confidencialidad, corresponde reafirmar lo que expresa el propio MSP en los fundamentos de creación del Certificado de Defunción en formato electrónico, respecto a la causa de la muerte: se trata de un dato clínico reservado en virtud de lo dispuesto en la Ley N° 18.335 sobre Derechos de los Pacientes y Usuarios, así como en la Ley N° 18.331 de Protección de Datos Personales.

En este sentido, la codificación de los datos clínicos contenidos en el mismo es un mecanismo idóneo para garantizar dicha reserva y confidencialidad.

-III- Sobre la validez legal del certificado electrónico del MSP sin intervención del Registro Civil La Dirección General del Registro del Estado Civil y las Intendencias Departamentales tienen la función de conservación, custodia, ordenado e indizado de los documentos que prueban el estado civil de las personas.

Estos documentos refieren tanto a hechos jurídicos o sea eventos cuyos efectos no resultan de la voluntad humana (nacimientos y defunciones), como a actos jurídicos o sea manifestaciones de voluntad dirigidas a producir determinados efectos (matrimonio, reconocimiento de la paternidad natural, el repudio de dicha paternidad, legitimación de hijos naturales por matrimonio, etc.), como a sentencias o resoluciones judiciales (divorcio, nulidad de matrimonio, etc.).

En definitiva, la función del Registro de Estado Civil es anotar los hechos o actos que atañen al estado civil, con la intervención de un funcionario público competente (Oficial del Estado Civil) en los libros correspondientes y con las formalidades que la ley prescribe.

Por ello, las copias autenticadas de las actas originales suscriptas por el Oficial del Estado Civil tienen validez legal, hacen plena prueba y poseen la eficacia de los instrumentos públicos.

En razón de ello, dicho certificado de defunción electrónico deberá contar con la intervención del Registro de Estado Civil, organismo que podrá hacerlo a través del sistema con firma electrónica avanzada, tal como se dispone en la Ley N° 18.600 de Documento Electrónico y Firma Electrónica (art. 6°), a efectos de otorgar la validez correspondiente.

-III- Sobre esquema de funcionamiento entre organismos y las formalidades del acuerdo de intercambio

Sobre el esquema de funcionamiento entre organismos, cabe tener presente lo ya expresado supra respecto a la finalidad de los datos y al cometido legal que tenga el organismo. Cuando los datos se comuniquen para cumplir con las funciones propias del organismo, o en virtud de una obligación legal, no se requiere recabar el previo consentimiento de los titulares (art. 9° C). Este sería el caso del BPS, por ejemplo.

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, las entidades u organismos que pretendan intercambiar información, por ejemplo MSP, Registro de Estado Civil o BPS, 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 emisor ante el jerarca del organismo receptor, y los acuerdos deberán establecer las condiciones, protocolos y criterios funcionales o técnicos con los que se llevarán a cabo dichos intercambios. 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).

-IV-Conclusiones

- a) En el caso, resulta aplicable el inciso B) del artículo 9° de la Ley N° 18.331 que exime de recabar el previo consentimiento informado de los titulares, cuando los mismos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.
- b) La excepción de recabar el previo consentimiento informado rige asimismo para la comunicación de datos que se desarrolle en el ámbito de los cometidos legales, no obstante, no es aplicable en el caso de que dicha comunicación se realice a otras entidades que no posean estos cometidos específicamente establecidos por Ley como por ejemplo el BROU.
- c) Los organismos involucrados podrán optar entre, celebrar un acuerdo de intercambio de información que establezca las condiciones, mecanismos y responsabilidades de cada uno; o de lo contrario adoptar los mecanismos o condiciones definidas por la AGESIC y formalizar un acuerdo en base a ello.
- d) En cuanto a la validez del certificado de defunción electrónico, éste deberá contar con la intervención del Registro de Estado Civil mediante el uso de la firma electrónica avanzada, a efectos de que posea la validez legal correspondiente.

Fdo. Dra. Graciela Romero

Derechos Ciudadanos

Informe N° 277, de 24 de mayo de 2012.

Se informa sobre consulta realizada acerca de adecuación de Resoluciones de la Administración de las Obras Sanitarias del Estado (OSE) a la Ley de Protección de Datos.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 277 | 12 | 2012-2-10-0000435 |

Montevideo, 24 de mayo de 2012.

Ref. Consulta OSE adecuación resoluciones a la Ley de PDP

-I- Antecedentes

Contenido de la consulta

El Esc. Horacio Urán solicita el pronunciamiento de la URCDP, respecto a cómo adecuar el contenido de las Resoluciones del Directorio de la Administración de las Obras Sanitarias del Estado (en adelante OSE), a lo establecido en la Ley N° 18.331 de Protección de Datos Personales, con la finalidad de ser publicadas en la web de dicho organismo público.

Expresa que OSE, con anterioridad a la creación de la Ley N° 18.381 de Acceso a la Información Pública decidió publicar, -a efectos de dar cumplimiento al deber de Transparencia ya establecido en el art. 7° de la Ley N° 17.060-, las Resoluciones del Directorio en su Página web, lo que ha venido haciendo hasta el presente.

Señala que, si bien la Ley N° 18.381 refiere al Principio de Transparencia de las entidades públicas, -y naturalmente OSE tiene obligación de cumplir con el mismo-, también es necesario procurar un balance o equilibrio con el derecho a la Protección de los Datos Personales establecido en la Ley N° 18.331.

Considerando las excepciones establecidas en los artículos 8° a 10 de la Ley N° 18.381, es que se consulta específicamente respecto a:

a) Que no deben publicarse los Sumarios Administrativos por tratarse de información reservada, y que el fundamento sería proteger la dignidad humana, establecido en el art. 9° inc. D) de la Ley N° 18.381.

b) Que no deben publicarse los datos personales que requieren previo consentimiento informado por constituir información confidencial, según lo establecido en el art. 10 de la Ley N° 18.381.

c) Que por remisión al art. 9° de la Ley N° 18.331 no se requiere el consentimiento en los casos que allí se mencionan, entonces como se está actuando en el ámbito de las excepciones en el caso los literales b) y d) del artículo 9° de la Ley N° 18.331, la información que contenga datos personales pese a ser confidencial o reservada, se puede publicar con los datos tanto de los funcionarios de OSE como particulares.

d) Si es correcto considerar que, si se toma en cuenta el principio de finalidad, establecido en el artículo 8° de la Ley N° 18.331, al publicar esos datos puede entenderse que se están empleando con un fin distinto, o excediendo el ámbito donde funcionan las excepciones, por

ejemplo se va mas allá del consentimiento genérico otorgado en virtud de la relación laboral o del ejercicio de las funciones propias de los poderes del Estado.

e) Si la publicación en la web de OSE de datos personales, -aún actuando dentro de las excepciones-, podría implicar una comunicación de los mismos según lo establece el art. 17.

f) Si para publicar habría que practicar un procedimiento de disociación de la información de modo que los titulares de los datos no fueran identificables. A modo de ejemplo, podría publicarse de la siguiente forma: "Visto la falta cometida por..... . "Disponer un Sumario Administrativo a....." "vista la situación del funcionario.....", "Disponer la realización de una Junta Médica al funcionario....."

En definitiva, se requiere un pronunciamiento de la URCDP a efectos de fijar criterios que permitan publicar las Resoluciones del Directorio de OSE en la página web del organismo, sin vulnerar el derecho a la protección de datos personales.

Corresponde tener presente antes de realizar este análisis jurídico, que no hay soluciones uniformes y globales que puedan abarcar la universalidad de hipótesis que eventualmente pueden plantearse en cada organismo público. Ello es así, porque la casuística es tan basta que siempre podrán plantearse dudas ante cada caso concreto, y en estos casos es conveniente consultar nuevamente la opinión de uno o de ambos Órganos de Control, o sea de la UAIP o la URCDP.

-II-Análisis

a) Sobre la reserva de los sumarios administrativos

En opinión de esta informante, mientras un Sumario Administrativo no se encuentre firme, debería ser clasificado como información reservada por parte del jerarca del organismo, indicando expresamente el fundamento de dicha reserva.

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 UAIP²¹: "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, en aras de proteger la dignidad de aquellas personas sometidas a un sumario administrativo, el expediente podría ser clasificado como reservado de acuerdo con el art. 9° D de la Ley N° 18.381. Dicha 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.

21 *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".*

Por otra parte, es importante tener presente, que también puede 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 (Principio de Divisibilidad).

b) Sobre la confidencialidad de ciertos datos personales

Según lo establecido en la Ley N° 18.331 art. 9°, 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.

Por otra parte, el literal b) del artículo 9° establece que no es 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 ese sentido, tomando en consideración los cometidos inherentes a OSE y su marco legal, cabe inferir que no se debe recabar el consentimiento de los clientes a efectos de cumplir con sus funciones o cometidos, así como para comunicar esos datos a determinados organismos públicos, siempre y cuando ello corresponda atendiendo a las funciones o cometidos de cada uno, a la finalidad del intercambio y a la regulación legal de dicho funcionamiento²².

Lo anterior en cambio, 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 es el interés del particular a la hora de brindar sus datos a un organismo público.

Por ello, ante un caso concreto que posee zonas grises, 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.

Además, hay que estar también a lo dispuesto por el Decreto Reglamentario N° 232/2010, reglamentario de la Ley N° 18.381, dónde se especifica cuál es la información que debe ser publicada por cada organismo en el cumplimiento de sus obligaciones de transparencia activa (art. 38).

De la descripción contenida en dicho Decreto, surge que hay ciertos datos que no deben ocultarse del conocimiento público, por ejemplo, los nombres de los funcionarios y sus méritos laborales o académicos, los nombres o la razón social de los titulares de concesiones, licencias, permisos y autorizaciones, así como de contratos que involucran el aprovechamiento de bienes, servicios o recursos públicos; y cualquier otro tipo de información, que pudiera ser de utilidad o relevante para el conocimiento y evaluación de las funciones y políticas públicas que son responsabilidad del sujeto obligado.

Además, de acuerdo a la Ley N° 18.331 hay 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.

22 Respecto al intercambio de información entre organismos públicos, estataleso no, se debe estar a lo dispuesto en los arts. 157 a 160 de la Ley N° 18. 719 de 27 de diciembre de 2010.

c) Sobre excepciones, principios y publicidad de los datos

Respecto a las cuestiones planteadas en los ítems c), d) y e), en el art. 17 de la Ley N° 18.331 sobre la comunicación de datos, se 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 lo que respecta a la existencia de una ley de interés general, es razonable interpretar que la Ley N° 18.381 de Acceso a la Información Pública debe ser considerada como tal, a efectos de garantizar la transparencia de la administración pública.

No obstante ello, siempre deben existir ciertos parámetros basados en la proporcionalidad y el equilibrio, a efectos de respetar y garantizar por igual, -en la medida de lo posible-, todos los derechos e intereses en juego.

Efectivamente tal como lo expresa el consultante, cuando se publican resoluciones que contienen todos los datos personales de los usuarios de los servicios de OSE puede interpretarse que los mismos se están empleando para una finalidad distinta a la que motivó su entrega, o excediendo el ámbito donde funcionan las excepciones, pues se va más allá del consentimiento genérico otorgado en virtud de la relación laboral o del ejercicio de las funciones propias de los poderes del Estado.

Es por ello justamente que, la Ley N° 18.331 se estructura en base a una serie de principios que 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).

Entre estos principios se encuentra el de finalidad (art. 8°), verdadero pilar de la protección de datos personales, que establece que los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles a aquéllas que motivaron su obtención.

Es así que los datos obtenidos para gestionar un trámite ante OSE, que es de interés de un ciudadano, deben ser utilizados para esa finalidad. Esto no significa de modo alguno, que una vez culminado el trámite, si hay resolución, ésta no deba ser publicada; por el contrario, debe ser publicada teniéndose presente que eventualmente ciertos datos no deberán estar incluidos, porque serían excesivos.

Esto quiere decir que los datos a publicar deben ser los necesarios, adecuados y proporcionales a la finalidad, que sería dar transparencia a la gestión pública.

En este sentido, también 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 del nombre, cédula de Identidad, nacionalidad, edad y dirección, 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.

La URCDP ya se ha pronunciado en este sentido, en el Dictamen N° 1/009 recaído en la Consulta sobre el Anteproyecto de Ley referido a la Publicidad de Certificados que otorga el

BPS²³. 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 hay casos en los que hay que ver si el contexto de la resolución revela otro tipo de información que afecta en forma desproporcionada la privacidad de una persona. O sea, no se puede incluir el nombre de una persona en una resolución que refiera a sus datos de salud, por ejemplo. En estos casos deben disociarse los datos.

Por ello, la otra solución es aplicar, para el caso de los datos de los particulares que obran en poder de los organismos, -y cuando ello corresponda-, las Reglas de Heredia²⁴ mediante un procedimiento de disociación (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 determinable²⁵.

En el caso de los funcionarios esto es diferente dado que se cumplen funciones para un organismo público, estatal o no, y hay que estar a lo dispuesto en el Decreto N° 232/010, reglamentario de la Ley N° 18.381. No obstante, aún en estos casos corresponde que la publicación también se limite a los datos que no requieren previo consentimiento informado, y a todos aquellos datos necesarios y adecuados para evaluar porqué se ocupa ese cargo o función. No se pueden publicar sin consentimiento por ejemplo, el estado civil, el teléfono particular del funcionario, si se tiene hijos o no, datos que indiquen su actividad política, el estado de salud, etc., porque sería excesivo y no adecuado a la finalidad.

La URCDP ya se ha expedido, respecto a que ciertos datos personales de los funcionarios pueden ser publicados. En el Dictamen N° 2/009²⁶, sobre publicación en la web de otras actividades laborales declaradas por Inspectores del M.S.P. el Consejo 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. De lo contrario, será necesario recabar el previo consentimiento informado, de acuerdo a las previsiones contenidas en el art. 9° de la LPDP.

En tanto en el Dictamen N° 2/010, respecto a la información que debe brindarse en el marco de los concursos públicos, la URCDP dictamina que en cuanto a la información que debe figurar en la página web (...) como forma de garantizar la transparencia activa del Organismo, (...), resulta suficiente la incorporación de los datos de quienes integren el orden de prelación (nombres y apellidos), junto con las puntuaciones globales de las respectivas etapas.

23 <http://www.datospersonales.gub.uy/sitio/dictamenes/2009/dictamen-1-009.pdf>

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

25 *Ver resolución N° 10/2009 de la UAIP de 3 de setiembre de 2009. <http://www.informacionpublica.gub.uy/sitio/consejo-resoluciones.html>*

26 <http://www.datospersonales.gub.uy/sitio/dictamenes/2009/dictamen-2-009.pdf>

Por último, en la Resolución N° 36/012, en denuncia presentada por una funcionaria contra UTU, el Consejo expresa que los teléfonos que aparecen publicados en la web de esta institución, no son los institucionales sino los particulares de cada docente y ello vulnera la Ley de Protección de Datos.

d) Sobre la disociación de datos personales

Como ya se ha expresado supra, una de las opciones a aplicar por parte de la OSE es la disociación de los datos personales. En este sentido, también el Consejo Ejecutivo de la URCDP ya se ha expresado en el Dictamen N° 15, de 15 de setiembre de 2011, ante consulta presentada por el Fondo de Solidaridad, que respecto 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.

Cabe decir que el ejemplo de resolución que se agrega a la consulta resulta adecuado. En este sentido, se considera lo ya expresado respecto a las Reglas de Heredia y lo establecido en el art. 10 de la Ley 18.381 art. 10 parte final, por lo cual cuando se trata de un archivo electrónico (para publicar) debe elaborarse la versión pública, eliminando las partes o secciones clasificadas como confidenciales.

-III-Conclusiones

1. La publicidad de los datos personales que no requieren el previo consentimiento informado, en el marco de las obligaciones de transparencia activa, no vulnera las disposiciones de la Ley N° 18.331, siempre que se hayan considerado los principios y excepciones previstas en la norma.
2. En este sentido, 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 los arts. 9° y 17 A) de la misma norma.
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. En el caso de los expedientes de sumarios administrativos, si bien éstos podrían ser clasificados como reservados una vez resuelto el asunto, debería brindarse acceso al contenido de la resolución en los términos ya mencionados.
5. Por otra parte, es importante tener presente que para proteger información que contenga datos personales, puede clasificarse sólo una parte de la misma considerándola confidencial, permitiendo el acceso a la parte que no lo es de acuerdo con el art. 10 in fine de la Ley N° 18.381.

Fdo. Dra. Graciela Romero
Derechos Ciudadanos

Informe N° 283, de 25 de mayo de 2012.

Se informa sobre consulta presentada por INMUJERES-MIDES sobre formación de base de datos de afrodescendientes.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 283 | 12 | 2012-2-10-0000448 |

Montevideo, 25 de mayo de 2012.

Ref. Consulta INMUJRES-MIDES formación base de datos de afrodescendientes

-I- Antecedentes

El Instituto Nacional de las Mujeres (INMUJERES) - Departamento de las Mujeres Afrodescendientes, del Ministerio de Desarrollo Social (MIDES), consulta sobre la formación e inscripción, de una base de datos territorial de profesionales y/o técnicos de origen afrodescendiente. A tales efectos, proporcionan la siguiente descripción de la referida base, así como los fundamentos de su creación:

a) Departamento de las Mujeres Afrodescendientes (INMUJERES, MIDES), es la dependencia encargada de gestionar su formación.

b) El método de recolección de datos se hará a través de un formulario digital auto-gestionado (se adjunta en archivo), que se ubica en el sitio Web del MIDES.

c) El espacio físico del soporte (el hosting y operación) de la Web MIDES, se gestiona mediante contrato realizado entre MIDES y la Empresa InnovaAge (se adjunta archivo con el contrato).

d) El fundamento para la creación de esta base, se encuentra en el mandato legal que se expresa en los Cometidos y Misión Institucional del MIDES (se adjunta archivo).

e) Los objetivos de la misma son fundamentalmente dos: a) Obtener una Base de Datos Territorial que sirva de justificación y fundamento para las Políticas Públicas, en especial las de Acción Afirmativa, y b) Evaluar los posibles avances que se han producido en dichas Políticas Públicas y su influencia en el colectivo Afrodescendiente (se adjunta archivo).

f) Por último, la fecha posible de lanzamiento o de inicio de la recolección de datos, está planificada para el mes de Junio.

La consulta refiere básicamente a si es legítima o no la recolección y tratamiento de datos que revelen el origen racial o étnico de las personas, -considerados datos sensibles-, por parte de este Departamento perteneciente al Ministerio de Desarrollo Social (MIDES), a la luz de lo establecido en el art. 18 de la Ley N° 18.331.

-II- Análisis

a. Sobre el alcance de la protección especial que se le otorga a los datos sensibles Como regla, los datos de origen racial o étnico, -por ser datos sensibles-, sólo pueden ser objeto de recolección y tratamiento con consentimiento expreso y escrito del titular o cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante

tenga mandato legal para hacerlo. También pueden tratarse con finalidades estadísticas o científicas, disociando los datos utilizados de sus titulares.

Este especial grado de tutela, adjudicado por las leyes de PDP, a los datos sensibles, tiene como objetivo evitar la discriminación.

El Principio de No Discriminación corta transversalmente todas las obligaciones asumidas por los Estados en materia de derechos humanos. En el ámbito regional, se encuentra expresamente reconocido en el art. 2.2 del Pacto Internacional de Derechos Económicos, Sociales y Culturales y en el art. 24 de la Convención Interamericana.

También es una obligación que surge a nivel regional del art. 3° del Protocolo de San Salvador, donde los Estados “se comprometen a garantizar el ejercicio de los derechos que en él se enuncian, sin discriminación alguna por motivo de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o racial, posición económica, nacimiento o cualquier otra condición social”.

No obstante ello, también existe la obligación a cargo de los Estados de actuar instrumentando las medidas y políticas necesarias y adecuadas, para garantizar y proteger los derechos humanos de todas las personas. Ello se denomina “discriminación positiva” e implica actuar con el fin de favorecer el desarrollo de los grupos y sectores de la sociedad que no tienen objetivamente las mismas posibilidades (“propendiendo a la consolidación de una política social redistributiva de carácter progresivo”, tal como se expresa en el DEC N° 286/006, de 22 de agosto de 2006 que se adjunta a la consulta)

Es razón de ello, determinadas entidades públicas, de acuerdo con sus fines y cometidos podrán mantener registro de este tipo de datos personales (planes de salud, planes de ayuda a personas con discapacidad, planes sociales, políticas de inclusión social dirigidas a minorías o grupos, etc.), lo cual significa que, si bien en principio está prohibida la creación de bases de datos sensibles, también hay excepciones que aluden en definitiva a razones de interés colectivo o de interés público.

En nuestro país, la Ley N° 18.331 en su artículo 18 establece 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.”

En el caso que se consulta, precisamente la finalidad de la base es servir de justificación y fundamento para las Políticas Públicas del MIDES, en especial las de Acción Afirmativa, así como evaluar los posibles avances que han producido a raíz de esas políticas públicas y su influencia en el colectivo Afrodescendiente.

b. Sobre los cometidos del MIDES e INMUJERES

La Ley N° 17.866 de creación del MIDES en el art. 6°, prevé que el Instituto Nacional de la Familia y la Mujer, se incorpore al Ministerio que se crea, manteniéndose su estructura y organización actuales y los recursos que tenga asignados.

En tanto en el art. 9° se establecen las competencias atribuidas al Ministerio de Desarrollo Social, -que a los efectos del tema analizado-, entre otras serían las siguientes:

- Asesorar al Poder Ejecutivo y proponer las políticas nacionales en las materias de su competencia.
- Formular, ejecutar, supervisar, coordinar, programar, dar seguimiento, evaluar las políticas, estrategias y planes en las áreas de juventud, mujer y familia, adultos mayores, discapacitados y desarrollo social en general.
- Coordinar las acciones, planes y programas intersectoriales, implementados por el Poder Ejecutivo para garantizar el pleno ejercicio de los derechos sociales a la alimentación, a la educación, a la salud, a la vivienda, al disfrute de un medio ambiente sano, al trabajo, a la seguridad social y a la no discriminación.
- Diseñar, organizar y operar un sistema de información social con indicadores relevantes sobre los grupos poblacionales en situaciones de vulnerabilidad, que permita una adecuada focalización del conjunto de políticas y programas sociales nacionales.
- Diseñar, organizar y administrar un sistema de identificación, selección y registro único de los núcleos familiares o individuos habilitados para acceder a los programas sociales, sujeto a criterios de objetividad, transparencia, selectividad, temporalidad y respetando el derecho a la privacidad en los datos que así lo requieran.
- Implementar, ejecutar y coordinar Programas de Atención a la Emergencia Social, mediante la cobertura de las necesidades básicas de quienes se hallan en situación de indigencia y de extrema pobreza, buscando el mejoramiento de sus condiciones de vida y su integración social.
- Proporcionar información y asesoramiento sobre los programas disponibles para quienes se encuentran en situación de indigencia o extrema pobreza.

c. Sobre el previo consentimiento informado y los cometidos del MIDES

El art. 18 de la Ley N° 18.331, establece que “ninguna persona puede ser obligada a proporcionar datos sensibles”, pero hace la salvedad de que “éstos podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular”. En el caso de la consulta, cada persona está brindando su consentimiento a la hora de llenar y enviar el formulario cuya copia se adjunta.

La Ley agrega además que: “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 disocian 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 en primer lugar la del consentimiento expreso y escrito del titular. Esto en definitiva, quiere decir que el consentimiento del titular enerva cualquier obstáculo y habilita su tratamiento.

En cuanto a la aplicación del principio del previo consentimiento informado cabe apuntar también, que atento a los cometidos asignados al MIDES, por la Ley de su creación N° 17.866 y normas posteriores, no sería exigible recabar el consentimiento informado de los titulares, en tanto éstos sean efectiva o potencialmente beneficiarios de sus programas, por resultar de aplicación el inciso B) del artículo 9° de la Ley N° 18.331, que exime de tal requisito cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

De todas formas, es importante tener presente que en el tratamiento de dichos datos, el Organismo deberá observar el cumplimiento del principio de veracidad, permitiendo que los datos sean adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se obtuvieron, así como del resto de los principios generales expuestos detalladamente en el Capítulo II de la LPDP, facilitando a las personas el ejercicio de los derechos de acceso, rectificación, actualización, inclusión o supresión, cuando proceda, y en forma gratuita.

La URCDP ya se ha expresado respecto a este tema en el Dictamen N° 11/010, de 7 de mayo de 2010, en la consulta del Ministerio de Desarrollo Social sobre criterios para el manejo de datos personales por parte del Organismo.

-III- Algunas recomendaciones

En primer lugar la base de datos deberá ser inscripta en el registro que lleva la Unidad Reguladora y de Protección de Datos Personales, tal como lo establece el art. 6° de la Ley N° 18.331.

En su operación además, se deberán observar los principios de Veracidad, Finalidad, Seguridad de los Datos, Reserva y Responsabilidad, así como lo establecido respecto a los derechos y obligaciones en general, especialmente lo formulado en el art.18.

En cuanto a la observación de las obligaciones establecidas en la Ley, al ser una base gestionada por una empresa ajena al Ministerio (como es el caso), en el contrato debería incluirse una nueva cláusula que delimite las responsabilidades, especialmente la obligación de reserva y confidencialidad que alcanza a todos quienes acceden y tratan esta información.

Es importante tener presente, que el personal de dicha empresa se encuentra sometido al deber de secreto, aún luego de concluida la relación laboral de acuerdo con lo establecido en el art. 11 de la Ley N° 18.331, y para ello se recomienda que todo el que realice el tratamiento, firme una cláusula de confidencialidad específica con el objeto de reforzar esta obligación.

Se recomienda a su vez, informar a los titulares en los términos establecidos en el art. 13 de la Ley, en el mismo formulario cuya copia se ha adjuntado, avisando a su vez del compromiso del responsable de utilizar esos datos de acuerdo con la Ley N° 18.331 y sin sentido o fines discriminatorios.

En tal sentido, se ha expresado la URCDP en el Dictamen N° 16/010 de 20 de agosto de 2010, en relación a una consulta sobre datos sensibles y referencias personales de las empresas de seguridad. Se agrega en dicho dictamen, que ello es así porque en la recolección y tratamiento de “datos sensibles”, además de informar en forma expresa, precisa e inequívoca al titular, se deben observar también criterios más severos que cuando se trata de datos personales comunes.

-IV- Conclusiones

1. Se considera legítima la recolección y tratamiento de datos que revelan el origen racial o étnico de las personas que se beneficiarán de las políticas o programas del Departamento de las Mujeres Afrodescendientes del INMUJERES, perteneciente al Ministerio de Desarrollo Social (MIDES), a la luz de lo establecido en el art. 18 de la Ley N°. 18.331.
2. La referida base de datos, deberá ser inscripta en el Registro de la URCDP dentro del plazo de 90 días, contados desde la fecha de su creación
3. Por otra parte, deberán adoptarse medidas de seguridad acordes así como observar el cumplimiento del resto de los principios y obligaciones previstas en la Ley.
4. Por último, para garantizar la confidencialidad y la reserva de los datos, es conveniente la inclusión de una cláusula adicional en el contrato celebrado entre MIDES y la Empresa InnovaAge, que establezca especialmente la obligación de reserva y confidencialidad que alcanza a todos quienes acceden y tratan esta información.

Fdo. Dra. Graciela Romero
Derechos Ciudadanos

Informe N° 271, de 17 de mayo de 2012.

Se informa sobre denuncia presentada contra institución bancaria por no proceder a eliminar su correo electrónico de la base de datos de marketing.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 271 | 12 | 2012-2-10-0000198 |

Montevideo, 17 de mayo de 2012.

Ref. Denuncia AA contra institución bancaria.

- I- Antecedentes

AA presenta denuncia online contra el BB, porque esta entidad no ha procedido a eliminar su dirección de correo electrónico de la base de datos de marketing.

La URCDP, para un mejor pronunciamiento procede a dar traslado de la denuncia a la empresa denunciada, quien toma vista y presenta sus descargos. A su vez, de los referidos argumentos se da vista al denunciante.

Una vez vencidos los plazos legales correspondientes, se procede a realizar informe jurídico de acuerdo a la legislación vigente en la materia.

-II- Análisis

El denunciante alega que ha presentado “varias solicitudes de remoción de la base de datos del Banco BB” sin haber obtenido respuesta. Agrega que acude a la URCDP, a efectos de que “intercedan para que se cumpla mi derecho a no figurar en la base de datos de dicha entidad bancaria”.

Adjunta copia del correo que ha enviado solicitando ser removido de la base, así como del último mail enviado por el Banco a su casilla de correo, confirmando la omisión a tal solicitud.

-III- Aspectos jurídicos a considerar

El artículo 4° literal D) de la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (en adelante LPDP) define al dato personal como “información de cualquier tipo referido a personas físicas o jurídicas determinadas o determinables”, en razón de ello cabe concluir que el correo electrónico es un dato personal cuyo tratamiento debe ser analizado a la luz de la ley antes mencionada y su reglamentación. Por otra parte, el art. 4° Literal C) 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”.

En tanto, el art. 21 de la Ley establece que: “en la recopilación de domicilios, reparto de documentos, publicidad, venta u otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento”.

El banco afirma en sus descargos que se le ha enviado publicidad al denunciante, porque éste se ha suscripto a su sistema Sucursal Internet, - cuestión que el denunciante no ha controvertido-, por ende, corresponde descartar que se haya vulnerado lo establecido en los artículos antes mencionados.

No obstante ello, tanto respecto a la obligación de informar al cliente, consagrada en el art. 13 E) de la Ley, como respecto a la obligación de garantizar el ejercicio de los derechos consagrados en los arts. 14, 15 y 21, cabe realizar las siguientes puntualizaciones:

a) En los casos de suscripción a sistemas de marketing electrónico debe ofrecerse, -por parte de quien habilita esta modalidad de publicidad-, al menos una posibilidad de exclusión en cada mensaje enviado. Dicha exclusión debería ser posible, como mínimo, utilizando el mismo servicio de comunicación (p. ej. enviando un mensaje SMS para ser excluido de una lista de marketing basada en un sistema SMS)²⁷.

En este sentido, si se ingresa a la página web de BB se ubica el formulario que se puede completar a efectos de que se envíe información de interés al correo electrónico que se proporcione. Debajo del mismo también puede leerse que se brinda la opción de borrarse, indicando “Estoy suscripto y quiero borrarame”.

En los descargos presentados, el banco indica que no había recibido ninguna solicitud “de baja por los mecanismos previstos a tales efectos”. El denunciante sin embargo, adjunta el correo que les ha enviado con fecha 18 de enero de 2012, solicitando ser removido de la base. El 6 de marzo de 2012 vuelve a recibir otra promoción del banco, lo cual prueba que no fue removido de la base tal como había solicitado mediante correo.

b) En cuanto al plazo para ejercer el derecho a ser retirado de dicha base, el banco indica en sus descargos que finalmente,- y debido al trámite realizado ante la URCDP-, el correo del denunciante ha sido eliminado del listado de suscriptores.

Por ende se ha cumplido con lo establecido en el art. 21 de la Ley, respecto a que el “titular de los datos podrá ejercer el derecho de acceso sin cargo alguno (...)”, así como “podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos a los que se refiere el presente artículo”.

Pero como el art. 21 no indica específicamente cuál es el plazo para garantizar este derecho, se debe realizar una interpretación amplia (por aplicación del Principio Pro Homine²⁸), y remitirse al plazo indicado en los arts. 14 y 15 de la Ley para el ejercicio de los demás derechos que se consagran, o sea 5 días. En definitiva, si bien el banco informa que ha cumplido eliminando los datos del denunciante, lo ha hecho en forma tardía.

27 Parte de la consideraciones vertidas por el G29 en el Dictamen N° del año 2004 sobre envío de comunicaciones en materia de venta directa. Ver: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_es.pdf

28 Mónica Pinto, *El principio pro homine. Criterios de hermenéutica y pautas para la regulación de los derechos humanos*, en LA APLICACIÓN DE LOS TRATADOS SOBRE DERECHOS HUMANOS POR LOS TRIBUNALES LOCALES 163, 163 (Martín Abregú & Christian Courtis eds., Editores del Puerto s.r.l. 1997) Definiendo el principio como “un criterio hermenéutico del cual se debe acudir a la norma más amplia, o a la interpretación más extensiva, cuando se trata de reconocer derechos protegidos e, inversamente, a la norma o a la interpretación más restringida cuando se trata de establecer restricciones permanentes al ejercicio de los derechos coincide con el rasgo fundamental del derecho de los derechos humanos [de] estar siempre a favor del hombre.”.

c) En cuanto al derecho a ser informado en los términos del art. 13 de la Ley, corresponde que al momento de la suscripción, figure una cláusula a efectos de recabar el consentimiento y que se informe claramente acerca de la finalidad de la base y los derechos que tiene el titular, (derechos de acceso, rectificación y supresión de datos). En este caso, también se debería informar acerca del mecanismo que se pone a disposición de los interesados para borrarse y cómo funciona.

-IV- Sobre la potestad sancionatoria de la URCDP

El Consejo Ejecutivo de la URCDP tiene potestades sancionatorias ante el incumplimiento de la Ley, pudiendo imponer sanciones que van desde la observación y el apercibimiento, hasta multa de hasta quinientas mil unidades indexadas y clausura de las bases de datos por un plazo de hasta seis días hábiles (artículo 35 de la LPDP en su redacción actual dada por la Ley N° 18.719, de 27 de diciembre de 2010 de Presupuesto Nacional del período 2010-2014). Este procedimiento se encuentra regulado en el artículo 31 del Decreto N° 414/009. Asimismo, el régimen sancionatorio encuadra dentro de la discrecionalidad que posee la Administración teniendo en consideración los principios de razonabilidad y proporcionalidad. Atento a ello, será el Consejo Ejecutivo de la URCDP quien podrá determinar las sanciones a imponer de acuerdo con la normativa vigente.

En el presente caso y conforme lo establecido ut supra, corresponde considerar que -según los descargos presentados por la empresa-, los datos del denunciante han sido eliminados con éxito de su base de datos. En la denuncia además, sólo se ha adjuntado un correo electrónico enviado por el banco luego de presentada la solicitud de baja.

Por otra parte, esta institución bancaria ya ha sido sancionada con anterioridad según surge de la Resolución N° 720/2011, de 14 abril de 2011, recaída en el Expediente N° 3030/2010. No obstante ello, de acuerdo a la Resolución de la URCDP N° 320/2011 deben considerarse como infracciones leves tanto el recolectar datos personales de los titulares, sin cumplir con el deber de informar que prevé el artículo 13 de la LPDP, así como no atender por razones formales a las solicitudes de los titulares de los datos cuando comparezcan a ejercer alguno de los derechos consagrados en la LPDP.

El banco a su vez, según informa en sus descargos, ha procedido a eliminar el correo de la lista una vez que la URCDP ha dado inicio a su actuación.

Hay que tener presente entonces, que no estamos ante una infracción grave de la Ley y que BB también tiene sus bases debidamente inscriptas en el Registro de la URCDP.

En base a todos estos elementos, se sugiere otorgar al BB un plazo de 30 días a efectos de que agregue en su sitio web, toda la información faltante de acuerdo a lo previsto en Ley N° 18.331, arts. 13, 14, 15 y 21 y analizada supra.

Se solicita otorgar vista previa al denunciado y denunciante, en los términos del art. 75 del Decreto N° 500/991, de 27 de setiembre de 1991.

Fdo. Dra Graciela Romero

Derechos Ciudadanos

Informe N° 270, de 18 de mayo de 2012.

Se informa sobre denuncia presentada contra un comercio por haber sufrido un hurto en ese local y éste no facilitar videograbación de local para la denuncia.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 270 | 12 | 2011-2-10-0000696 |

Montevideo, 18 de mayo de 2012.

Ref. Denuncia AA contra BB

-I- Antecedentes

La denunciante comparece manifestando haber sufrido un hurto de su billetera con los documentos mientras hacía un pago en la caja de una de las sucursales de Supermercados BB, denunciando a esta empresa por no facilitarle las videograbaciones del local donde ocurrió el hecho.

-II- Análisis

Salvo mejor sugerencia, corresponderá declinar competencia en cuanto al objeto central de la denuncia presentada, asesorando a la denunciante acerca de la vías y acciones jurídicas de que dispone para satisfacer su interés de "ver quién y cómo me robaron" según es su propósito declarado.

Concomitantemente se sugerirá, también, ordenar a la empresa denunciada la inscripción de la base de datos referida a actividades de videovigilancia, y la colocación visible de los logos correspondientes conforme Resolución N° 989, de 30 de Julio de 2010 de la Unidad, mediante intimación con plazo de 30 días, bajo apercibimiento de ser sancionada.

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 318, de 6 de junio de 2012.

Se informa sobre consulta acerca de la legalidad de la comunicación de datos realizada por parte del Fondo de Cesantía y Retiro de la Construcción (FOCER).

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 318 | 12 | 2012-2-10-0000467 |

Montevideo, 6 de junio de 2012

Ref. Consulta FOCER

-I- Introducción

El Fondo de Cesantía y Retiro de la Construcción (FOCER), es un órgano que brinda una prestación a los trabajadores de la construcción en ocasión, de cese, retiro, o en casos extraordinarios. Consiste en un sistema de ahorro individual para los trabajadores del ramo, formado con aportes patronales y de los trabajadores, por lo cual cada trabajador tiene su cuenta individual.

La consulta refiere a la legalidad de la comunicación de datos personales que debe realizar dicha institución a Cambio Gales Servicios Financieros SA y a Western Union, debido a que estos datos pertenecen a trabajadores de nacionalidad argentina que gestionaron dicho beneficio pero luego se marcharon nuevamente a ese país. Cuando el dinero estaba a su disposición para el cobro, se instrumentó la realización del giro del dinero a cada uno de ellos, a través de Gales Servicios Financieros S.A y Western Union.

Sin embargo, Cambio Gales expresa que para poder realizar los giros necesitan registrar a la empresa que remite los mismos, y además deben contar con un respaldo que explique el porqué de cada giro, ante la eventualidad de que el Banco Central les solicite esa información. Si bien Cambio Gales expresa que esa información será totalmente confidencial por ser una institución regida por las normas del secreto bancario, -sólo pudiendo ser divulgada en caso de que el Banco Central o Western Union se las solicite-, se consulta acerca de si la comunicación de datos personales que se debe realizar, -sin recabar el previo consentimiento de los interesados por estar en Argentina-, se ajusta a lo establecido en la Ley N° 18.331.

-II.- Sobre las excepciones al consentimiento

El artículo 17 de la Ley 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. Agrega que éste último, no será necesario en una serie de excepciones que se enumeran. En lo que respecta a este análisis, nos detendremos en lo establecido en el inciso B), que nos remite a su vez a los supuestos del artículo 9° de la ley.

En el caso que se consulta evidentemente existe interés legítimo, tanto del emisor como del destinatario. Veamos qué sucede con el consentimiento.

Como ya se ha expresado, el art. 17 remite al art. 9° de la Ley, donde se establece que “no será necesario el previo consentimiento cuando... B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal”.

En el caso, se trata de datos personales que constituyen un insumo para cumplir con las obligaciones que por ley se le asignan a las instituciones financieras. Efectivamente, tanto la Ley N° 17.835 sobre Sistema de Prevención y Control del Lavado de Activos y de la Financiación del Terrorismo, en su redacción dada por la Ley N° 18.494, como su Decreto reglamentario, imponen a los sujetos obligados el relevamiento, registro y conservación de datos personales de personas físicas y jurídicas.

Por su parte, el Decreto reglamentario N° 355/010, establece la obligación de todos los sujetos obligados a cumplir e implementar las disposiciones del decreto y las reglamentaciones que emitan sus respectivos organismos de control o el Banco Central del Uruguay, las que comprenderán entre otras: el registro de transacciones que con ellos se realicen y la conservación de los documentos que acrediten las mencionadas transacciones.

Ello implica el relevamiento y conservación, por parte de los sujetos obligados de abundante información personal de sus clientes, ya sean personas físicas (nombre y apellido completo; fecha y lugar de nacimiento, documento de identidad, estado civil y datos del cónyuge, domicilio, profesión o actividad, volumen de ingresos) o jurídicas (denominación, fecha de constitución, nombre y documento de los socios o accionistas, directores, copia autenticada del contrato social y número de RUT); búsqueda de antecedentes de las personas físicas o jurídicas en fuentes públicas o privadas; información sobre el propósito y la naturaleza de la relación.

En definitiva corresponde aplicar al caso, la excepción prevista en el art. 9° B) que habilita la comunicación de datos personales sin el previo consentimiento informado de los titulares, en razón de la existencia de un marco legal que determina una serie de obligaciones que deben cumplir las instituciones involucradas en la transacción financiera.

Por otra parte, el art. 9° D) de la Ley N° 18.331, establece otra excepción al consentimiento cuando los datos “deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento”.

En el caso, los datos personales de los trabajadores deben ser comunicados para cumplir con el pago de los beneficios solicitados por ellos y cumplir así con las obligaciones surgidas en el marco de un contrato celebrado entre FOCER y esos trabajadores, por ende debe considerar también la aplicación de esta excepción.

-III- Sobre la observancia de los demás principios de la Ley

A pesar de la aplicación de las excepciones al consentimiento ya analizadas, corresponde tener presente, los demás principios que inspiran la protección de datos personales, sobre todo y especialmente los de finalidad, confidencialidad y seguridad, los cuales a su vez, servirán de criterio interpretativo para resolver las cuestiones que puedan suscitarse.

En definitiva, si bien desde el punto de vista del régimen jurídico de la protección de datos personales no existen impedimentos para dar curso a dicha comunicación de datos en los

términos establecidos en la consulta, es importante tener presente que aún respecto a aquellos datos que no requieren previo consentimiento informado, FOCER deberá observar los demás principios que estructuran la Ley, así como garantizar el ejercicio de los derechos consagrados en la misma.

-IV- Conclusiones

a) En el caso resultan aplicables las excepciones previstas en los incisos B) y D) del artículo 9° de la Ley N° 18.331 que eximen al consultante de recabar el previo consentimiento informado de los titulares cuando los mismos se recaben o comuniquen en virtud de una obligación legal o cuando deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

b) Las entidades involucradas están obligadas a observar los demás principios que estructura la Ley N° 18.331.

Fdo. Dra. Graciela Romero

Derechos Ciudadanos

Informe N° 336, de 13 de junio de 2012.

Se informa sobre denuncia contra organismo público por no corroborar la identidad y otorgar un contrato por error a otra persona de igual nombre.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 336 | 12 | 2012-2-10-0000254 |

Montevideo, 13 de junio de 2012.

Ref. Denuncia contra BB y CC

-I- Antecedentes

AA denuncia a BB y CC porque al solicitar un teléfono nuevo, en el marco de un contrato con el Plan CC, la persona que la atiende en BB le informa que no puede otorgárselo, porque ya había realizado otro el 8 de febrero de este año en Maldonado, y el contrato CC solo puede solicitarse una vez.

Para averiguar su situación se dirige al Departamento Comercial de BB, a efectos de reclamar y exigir que corroboraran sus datos. Luego de su gestión, BB le da de baja respecto al contrato con el que figuraba, así como le explican que había ocurrido un error de tipeo que originó que hicieran un contrato con su documento de identidad, pero a nombre de otra persona que se llama igual que ella y vive en Maldonado.

En la denuncia, AA también reclama acceder a la siguiente información: quiere saber si está en el sistema y si está por qué razón, así como obtener copia del contrato, cuándo, a quién, dónde, el registro de su reclamo, la solución y lo que se hizo para solucionar el problema.

La URCDP para un mejor pronunciamiento da vista a las empresas involucradas.

CC toma vista pero no presenta aclaraciones, en tanto BB presenta sus argumentos afirmando que ha dado cumplimiento a uno de los extremos reclamados por la denunciante.

De los referidos argumentos se da vista a la interesada mediante correo electrónico, pero pasado el plazo correspondiente no presenta nuevas aclaraciones.

-II-Argumentos de BB

Este organismo afirma que una vez recibido el reclamo se constató que, al poseer en la base los datos de varias personas que tienen el mismo nombre y apellido, por error se cargó el contrato a nombre de la denunciante, pero una vez recibido el reclamo se procedió a subsanarlo en forma inmediata.

Agrega que en ningún momento se han vulnerado los datos personales de AA, pero no aportan más información relativa a la denunciante.

-III- Análisis de la denuncia presentada

La denuncia tiene dos aspectos a ser considerados:

1- El error que llevó a que un funcionario de BB le adjudicara a AA un contrato que no tenía.

2- La solicitud de acceso a determinada información personal que posee BB respecto de la denunciante.

Respecto al primer punto, cabe concluir que según los argumentos presentados por BB, -y que la denunciante no ha controvertido-, una vez recibido el reclamo y constatado el error, se ha procedido a subsanar el mismo en forma inmediata.

En cuanto a la posibilidad de ejercer los derechos de rectificación, actualización o supresión por parte del denunciante, es oportuno tener presente que el art. 15 de la Ley establece que “Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad (...)”.

Respecto al segundo punto cabe realizar las siguientes puntualizaciones:

El art. 14 de la Ley establece que “Todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas”.

En razón de ello y estudiados los argumentos de BB, cabe concluir que correspondería solicitar a este organismo, que proporcione en el plazo que determine el Consejo, toda la información que posee sobre la denunciante en sus bases de datos, incluyendo todo lo relacionado con este incidente, el trámite de su reclamo y la solución adoptada, salvaguardando los datos personales de los terceros ajenos al mismo.

-IV- Conclusión

En síntesis, si bien cabe inferir que ha existido por parte de BB un tratamiento de datos personales originado en el error de un funcionario, también surge que este organismo ha sido omiso al garantizar el derecho de acceso previsto en el art. 14 de la Ley.

Con la finalidad de que se garantice este derecho se recomienda otorgar un plazo razonable para que se haga entrega a la denunciante de toda la información solicitada.

Fdo. Graciela Romero
Derechos Ciudadanos

Informe N° 408, de 22 de junio de 2012.

Se informa consulta acerca de la adecuación a la Ley N° 18.331 del sistema de denuncia en línea del Ministerio del Interior.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 408 | 12 | 2012-2-10-0000679 |

Montevideo, 22 de junio de 2012

Ref. Consulta sobre adecuación sistema de denuncia en línea del Ministerio del Interior

-I- Introducción

La consulta busca recabar la opinión de la URCDP respecto a:

a) Formulario elaborado para recabar el consentimiento para el tratamiento de los datos personales de los involucrados.

b) Sobre el consentimiento del personal: “Deben incluirse en la oferta, los currículums vitae del personal propuesto. En este caso, como el oferente deberá recabar el consentimiento de los titulares de los datos personales contenidos en la propuesta, se consulta acerca de si la certificación de dicho consentimiento se puede presentar mediante la firma de los titulares en su respectivo currículum o es necesario presentar carta complementaria”.

-II- Sobre el formulario

No se presentan objeciones respecto a ninguno de los puntos ahí señalados, salvo recomendar que se elimine la expresión “cualquier forma de...”, quedando redactado de la siguiente manera: “...manifiesta que consiente la utilización, comunicación...”.

-III- Sobre el consentimiento del personal a cargo del oferente

La URCDP ya se ha expedido respecto a este tema en consulta similar, mediante el Dictamen N° 17/010 de 20 de agosto de 2010 (Expediente N° 009/2010).

Conforme al artículo 9° de la LPDP, la persona que se postula a un llamado laboral y entrega su Curriculum Vitae a su empleador, ya está prestando su consentimiento de forma documentada, libre, previa, expresa e informada. En el momento en que presenta el Curriculum Vitae para postular a ese empleo, el titular conoce la finalidad para la cual se destinarán los datos y el tipo de actividad desarrollada por su empleador, por lo cual se infiere que este tipo de tarea a desarrollar en el marco de esta licitación, está en consonancia con el principio de finalidad establecido en el artículo 8° de la LPDP.

En este caso además, debe considerarse lo expresado en el artículo 17 de la Ley que 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, pero agregando que éste último, no será necesario en una serie de excepciones que se enumeran. En lo que respecta a este análisis, nos detendremos en lo establecido en el inciso B), que nos remite a su vez a los supuestos del artículo 9° de la ley.

En el caso evidentemente existe interés legítimo, tanto del emisor como del destinatario. En cuanto al consentimiento, el art. 9° D) de la Ley establece la excepción al consentimiento cuando los datos “deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento”.

En el caso consultado los datos personales de los trabajadores deben ser comunicados para cumplir con tareas y obligaciones surgidas en el marco de un contrato laboral celebrado entre el oferente y sus trabajadores.

- IV- Conclusión

En definitiva, considerando lo ya expresado por la URCDP en anterior dictamen y analizando las circunstancias planteadas en la consulta, cabe concluir que no sería necesario recabar el previo consentimiento, sin perjuicio de que dichos oferentes tienen el deber de informar a quienes se incluyen en la licitación, en los términos establecidos en el art. 13 de la Ley.

Respecto a las obligaciones del organismo o institución que debe controlar los pliegos de condiciones de las licitaciones, se debe considerar que no corresponde el control de tal requisito, pues éste refiere a las actividades propias de quienes son los responsables de las bases de datos o del tratamiento de los datos personales de los trabajadores con quienes mantienen el vínculo laboral.

Fdo. Dra. Graciela Romero
Derechos Ciudadanos

Informe N° 337, de 13 de julio de 2012.

Se informa sobre consulta del Ministerio de Educación y Cultura, Dirección General de Registro de Estado Civil, sobre solicitudes de datos que recibe de otros organismos públicos o privados.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 337 | 12 | 2012-2-10-0000586 |

Montevideo, 13 de julio de 2012

Ref. Consulta Ministerio de Educación y Cultura. Dirección General de Registro de Estado Civil.

I. Introducción.

La Dirección General de Registro de Estado Civil (DGREC) formula consulta a la Unidad Reguladora y de Control de Datos Personales (URCDP), sobre las solicitudes de datos que recibe de organismos públicos y privados respecto a la información contenida en sus bases de datos.

Se consulta acerca de si se encuentran habilitados a proporcionar la información requerida y en caso afirmativo con que alcance debe proporcionarse.

En virtud de la consulta recibida y en cumplimiento de las facultades que le son otorgadas a la URCDP por el artículo 34 de la Ley, la Unidad procede a la sustanciación de ésta.

II. Análisis de la consulta.

II.a. De las bases de datos llevadas por DGREC.

A efectos del encuadre de la presente consulta resulta pertinente referir a las disposiciones legales y reglamentarias que tienen relación directa con el tema.

En primer lugar, debemos referir al Decreto-Ley N° 1.430 promulgado el 12 de Febrero de 1879 por la cual se crea el Registro especial llamado "Registro del Estado Civil" para la comprobación del Estado Civil de las personas. Este Registro comprende: El de los nacimientos, el de los matrimonios, el de las defunciones, y el de reconocimiento.

La mencionada norma indica los elementos comunes que deben mencionarse en los asientos realizados en los libros que llevan los diversos registros como: el lugar, año, mes, día y hora en que se hacen; los nombres, apellidos, edad, sexo, estado, profesión, nacionalidad y residencia de los interesados y de los testigos que intervienen en los asientos; todas las demás disposiciones exigidas por la ley.

Por otra parte, la ley se encarga de referirse a los datos que deben incluirse, además de los mencionados, en cada uno de los Registros en forma particular.

II.b. Aplicación de la normativa de protección de datos personales a las bases de datos llevadas por DGREC.

En este punto cabe analizar si a las bases de datos llevadas por la Dirección General de Registro de Estado Civil le son aplicables las disposiciones de la Ley N° 18.331, de 11 de

agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP).

La respuesta a la interrogante aparece dada por lo dispuesto en el literal C) del artículo 3° de la mencionada norma, que respecto a su ámbito objetivo de aplicación, excluye de éste a las bases de datos creadas y reguladas por leyes especiales, como es el caso de las que lleva la consultante.

Por otra parte, se estima pertinente mencionar las previsiones contenidas en los artículos 9° y 17 de la Ley, que se encargan de regular las disposiciones relativas al consentimiento informado indicando que éste no será necesario cuando los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de información.

Igualmente debe tenerse presente que la información que se encuentra en el Registro de Estado Civil, ha sido incluida en éste en cumplimiento de una finalidad determinada asociada a la comprobación del Estado Civil de las personas. Por ello corresponde indicar que no es posible que la información allí contenida sea comunicada en forma indiscriminada o excesiva, perdiendo de vista la finalidad para la cual fue recabada la información. El acceso a la totalidad de la base de datos podría ser violatorio de los principios generales en materia de protección de datos personales o violentar los derechos de otras personas. Por ello, debe analizarse en cada caso la pertinencia de la solicitud y de la información que se pretende obtener.

Además de lo expuesto, se deben tener presentes otras normativas en materia de filiación que puedan establecer limitaciones o reservas frente a determinadas partidas de estado civil.

III. Conclusiones.

1- De acuerdo a lo establecido por el literal C) del artículo 3° de la Ley N° 18.331, de 11 de agosto de 2008 no se aplica el régimen de la Ley a las bases de datos llevadas por el Registro de Estado Civil.

2- Analizar la pertinencia de cada solicitud teniendo en cuenta la finalidad para la cual se han recabado los datos, permitiendo el acceso únicamente a aquellos elementos que sean solicitados y no a la totalidad de la base de datos, caso en el cual podrían violentarse los principios generales de la protección de datos.

3- Tener en cuenta las previsiones de otras leyes especiales.

Fdo. Dra. Jimena Hernández

Derechos Ciudadanos

Informe N° S/N, de 26 de julio de 2012.

Se informa sobre alcance del artículo 291 del Proyecto de Ley de Rendición de Cuentas y Balance Presupuestal – Ejercicio 2011, que refiere a la posibilidad de mantener los datos inscriptos en la Central de Riesgos, una vez vencidos los plazos correspondientes.

| INFORME No. | | ACTA No. |
|-------------|----|----------|
| s/n | 12 | 29 |

Montevideo, 26 de julio de 2012.

Ref. Análisis artículo 291 del Proyecto de Ley Rendición de Cuentas y Balance de Ejecución Presupuestal- Ejercicio 2011.

-I- Introducción

ARTÍCULO 291.- "Incorpórase al artículo 2 de la Ley No.18.812, de 23 de setiembre del 2011, el siguiente inciso a continuación del primero:

"Sin perjuicio de lo dispuesto en el inciso precedente, una vez transcurrido el plazo para que los datos permanezcan inscriptos en la Central de Riesgos Crediticios, el Banco Central del Uruguay podrá mantenerlos como datos estadísticos con el único fin de realizar estudios de riesgo de crédito para el desarrollo de sus funciones de regulación, adquiriendo tales datos, en este caso, carácter confidencial".

El análisis del artículo propuesto refiere a varios aspectos a considerar:

- a. Qué tipos de datos serán conservados.
- b. Los plazos existentes para que los datos permanezcan inscriptos en la Central de Riesgos Crediticios.
- c. Que el Banco Central del Uruguay pueda mantenerlos más allá del plazo como datos estadísticos con el único fin de realizar estudios de riesgo de crédito.
- d. El carácter de confidencialidad que adquieren esos datos en tales casos.

-II-Análisis

- a. ¿Qué tipo de datos posee la Central de Riesgos Crediticios?

Para comenzar este análisis es importante tener en cuenta el tipo de información o de datos que contiene la Central de Riesgos Crediticia. Se trata de datos personales de carácter comercial o crediticio, cuyo acceso actualmente se encuentra habilitado por un sistema de auto-consultas públicas (al que se ingresa sólo con el Número cédula de Identidad propia o ajena), y que permite recuperar información sobre las deudas de todas las personas, así como la calificación que le ha sido otorgada de acuerdo a los parámetros establecidos por la normativa del Banco Central.

La referida información, que se puede extraer del sistema simplemente ingresando al mismo, está dispuesta y regulada por el art. 22 de la Ley N° 18.331 dentro del capítulo IV o sea que se trata de datos especialmente protegidos. Lo que hace la norma, -y así lo dice expresamente el art. 22-, es autorizar su tratamiento consagrando en definitiva un régimen excepcional (Informe N° 1533 del Dr. Marcelo Bauzá. Expediente 1955/2010).

Por otra parte, el sistema de auto-consultas no sólo contiene datos personales actuales sino también históricos, para lo cual se establece una relación entre diferentes deudas y plazos, todo ello sumado a la calificación otorgada.

En definitiva, en nuestra opinión a efectos de no vulnerar lo establecido en el art. 8° de la Ley, en el caso concreto y en la hipótesis de su conservación única y exclusivamente para fines estadísticos (tal como se establece en el artículo 291 propuesto), esta información debería conservarse en forma disociada de sus titulares, al amparo de lo previsto por el literal D) del artículo 17 de la LPDP.

b. Sobre los plazos de conservación que aplican a la Central de Riesgos Crediticios Según la Ley N° 18.331, los plazos para conservar este tipo de información especialmente protegida son los establecidos en el art. 22. Es así que se establece un registro inicial por 5 años, susceptible de renovarse solamente por otros 5 años. Siempre y cuando el acreedor lo pida dentro de los 30 días anteriores al vencimiento del plazo inicial estando vigente la deuda. Por otra parte, las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, que se cuenta desde la fecha de la cancelación.

En cambio, mediante la Ley No.18.812, de 23 de setiembre del 2011 sobre Datos de Carácter Personal inscriptos en la Central de Riesgos Crediticios del Banco Central del Uruguay, se ha modificado el plazo previsto en este régimen especial, estableciendo uno en forma específica y separada para esta base de datos.

Justamente en el artículo 2° (Plazo de registro), se establece que los datos personales relativos a personas físicas podrán permanecer inscriptos en la Central de Riesgos Crediticios a cargo del Banco Central del Uruguay, por un plazo máximo de quince años contados a partir del vencimiento de la operación.

Actualmente entonces, mediante el art. 291 analizado, se propone incorporar a ese artículo 2° otro inciso donde se autoriza a mantener sin límite de tiempo la información ahí registrada, o dicho de otro modo esos datos personales permanecerán inscriptos en la Central de Riesgos Crediticios del BCU a perpetuidad.

Esto significa en realidad, excepcionarse nuevamente de aplicar la norma que habilita el tratamiento en forma excepcional de este tipo de información (art. 22). También implica no aplicar uno de los Principios que rigen para el sistema de Protección de Datos, el de Finalidad, en lo que respecta a lo establecido en el art. 8°: "Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados".

Al respecto, como ya se ha expresado por parte de la URCDP, creemos que continuar con una postura de excepcionamiento del régimen de protección integral de un derecho, que construye la Ley N° 18.381 en el marco del artículo N°72 de la Constitución, tiene consecuencias negativas para el sistema de garantías que se ha pretendido instaurar en el país.

Citando nuevamente al Dr. Marcelo Bauzá, en el informe ya mencionado, se vuelve a dejar "a la deriva, sin los límites requeridos para su renovación temporal, permitiendo a través de este descontrol unas vigencias registrales por tiempos mayores a los permitidos por la ley (art.

22 de la Ley No. 18.331), y la no eliminación de los registros en el momento y tiempo legal dispuestos para ello (art. 15 de la Ley No. 18.331)".

-III- La conservación más allá de estos plazos pero como datos estadísticos

Decíamos que mediante el artículo propuesto se autoriza a que el Banco Central del Uruguay conserve este tipo de datos más allá de los plazos antes mencionados.

Se agrega en el proyecto de artículo, que esos datos se conservarán como datos estadísticos con el único fin de realizar estudios de riesgo de crédito para el desarrollo de sus funciones de regulación. Este punto se relaciona directamente con lo ya expresado respecto a que esa información debería conservarse en forma disociada de sus titulares, al amparo de lo previsto por el literal D) del artículo 17 de la LPDP.

Por ende, si ello fuera así, esas estadísticas sólo podrán utilizarse para realizar "estudios de riesgos de crédito" en forma genérica y no personalizada. Dicho de otra forma: no podría analizarse por parte del BCU cuántas veces se atrasó una persona en sus pagos, cuántas veces fue calificado con el grado 5, por lo cual si es conveniente o no autorizarle un crédito en base a esas estadísticas, etc., justamente porque los datos se han conservado en forma disociada a su titular.

Si ello no es así, además del art. 8° de la Ley también se vulnera lo establecido en el art. 16 (Derecho a la impugnación de valoraciones personales), que consagra el derecho del titular del dato a no ser evaluado mediante tratamientos automatizados o no, destinados a evaluaciones personales de distinto tipo, que lo afecten de manera significativa.

En este caso, justamente porque las calificaciones que otorga la Central de Riesgos Crediticia, se basan en la construcción de un perfil comercial o económico de una persona, que se traducen en definitiva en una verdadera valoración personal, agravada en muchos casos por el hecho de esa calificación puede llegar a ser muy negativa para su imagen, es que debemos ser extremadamente cuidadosos con el tiempo de conservación de los datos.

Esa calificación en definitiva es una valoración personal realizada desde un punto de vista comercial y crediticio, que sin lugar a dudas, -en caso de ser negativa-, afecta la imagen y las posibilidades de desarrollo y crecimiento de una persona. Si la información en este caso, es conservada asociada a su titular, a ello habría que sumarle el hecho de que la misma podría mantenerse sin límite de tiempo y alimentarse con datos que se van recopilando a lo largo de toda la vida del ser humano.

En estas hipótesis estamos ante casos, donde la garantía de la vida privada de la persona y su reputación poseen una dimensión positiva que se traduce en el derecho a tener el control sobre sus propios datos personales, sobre su uso y destino, así como del tiempo que se conservarán, con el propósito legítimo de impedir que su tratamiento sea lesivo para la dignidad del afectado.

Estamos además, ante un derecho específico que se deriva de lo anterior y se abre paso con mucha fuerza, el denominado "derecho al olvido". Este derecho, -que es en realidad una aplicación del actual derecho a la cancelación, supresión u oposición-, enfatiza en que los responsables del tratamiento están obligados a suprimir los datos de los interesados que así lo soliciten.

- IV- Sobre el carácter de confidencialidad que adquieren esos datos en tales casos

Éste es el punto que más debe preocuparnos. Es claro que el actual sistema de funcionamiento de la Central de Riesgos Crediticia de nuestro país no brinda el carácter de confidencialidad a la información que contiene, debido a que cualquier persona, con su cédula de Identidad o con el número de otra, puede acceder a través del sistema de auto-consultas público.

Lo que se establece en el inciso que se proyecta incorporar a la Ley N° 18.812, es que pasados el plazo de 15 años establecidos en la misma, los datos serán conservados por el BCU, pero en tales casos tendrán el carácter de información confidencial.

Si bien ello está en consonancia con lo establecido en el art. 10 Núm. II de la Ley N° 18.381 de Derecho de Acceso a la Información Pública, que señala que los datos personales que requieren previo consentimiento informado deben ser considerados información confidencial, debemos preguntarnos por qué se van a conservar con tal carácter si se mantienen disociados y se utilizarán sólo para generar información estadística.

En el caso de que se mantengan asociados al nombre de sus titulares, sí tiene sentido que se aclare que tendrán esa calidad, sobre todo para indicar que ya no serán objeto de las consultas públicas realizadas a través del sistema que actualmente se habilita.

En definitiva, si se conservaran disociados de sus titulares sólo para fines estadísticos no deberían ser considerados confidenciales por su carácter de dato personal. Cuando el dato no se vincula al nombre de la persona, no permitiendo su identificación, pierde el carácter de dato personal y no se requiere el consentimiento del titular para el tratamiento.

Este punto entonces no es claro (o sí lo es, depende de la intención de la norma) por lo cual, a nuestro modo de ver, es uno de los puntos que permite deducir que los datos no estarán disociados.

-V- Conclusión

Se sugiere a la URCDP, en el marco de sus cometidos consagrados en el art. 34 D) de la Ley N° 18.331, solicitar al BCU que aporte información acerca de:

1- Si los datos serán conservados más allá de los plazos legales establecidos, en forma disociada de sus titulares, al amparo de lo previsto por el literal D) del artículo 17 de la misma norma.

2- El alcance de la finalidad expresada en la frase: con el único fin de realizar estudios de riesgo de crédito para el desarrollo de sus funciones de regulación.

Fdo. Dra. Graciela Romero

Derechos Ciudadanos

Informe N° 391, de 26 de julio de 2012.

Se informa sobre denuncia contra periódico barrial por publicación de datos personales de funcionarios del complejo de viviendas.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|--------------------|
| 391 | 12 | 2012-02-10-0000451 |

Montevideo, 26 de julio de 2012

Ref. Denuncia AA y otros c/ BB

-I- Antecedentes

Varias personas presentan denuncia contra BB, editor de un periódico barrial, por entender que el mismo ha vulnerado la Ley de Protección de Datos Personales, al utilizar sin su consentimiento, sus nombres e información relacionada con ellos en ese medio de difusión.

La URCDP para un mejor pronunciamiento, procede a dar traslado de la denuncia y demás aclaraciones a ambas partes, quienes presentan sus descargos en tiempo y forma. Una vez vencidos los plazos legales otorgados se realiza el informe jurídico correspondiente.

-II- Análisis de los argumentos presentados

Los denunciantes son funcionarios del Complejo Habitacional ubicado en ese barrio. En su denuncia informan que con fecha 15 de junio de 2011, habrían enviado una nota al editor responsable del periódico a efectos de solicitarle que no publicara más sus datos personales (sus nombres y otros datos que no se identifican por los denunciantes pero se presume que se relacionan con la información que se intercambia en las asambleas).

Agregan que, si bien BB es Presidente de unos de los bloques del Complejo, el periódico es un emprendimiento privado de carácter comercial, por esa razón ellos no autorizan que sus datos personales sean utilizados en el mismo. Agregan que además, esa utilización ha generado una opinión que los perjudica, hiere su integridad y su sensibilidad.

Aclaran que el complejo ya tiene un boletín oficial que es emitido por la Mesa Central en representación de la Asamblea de Gobierno y Administración, máximo órgano de administración y control del conjunto habitacional. Este boletín se financia con fondos de todos y brinda información de carácter objetivo sin fines comerciales. Agregan que ellos no se oponen a que sus datos se traten en este boletín.

BB por otra parte, aduce que es Editor Responsable de un órgano de prensa independiente, registrado en el MEC (N° XXXX, Tomo XV a fojas 81). Que se trata de una publicación mensual, integrada por un Consejo Editor de carácter honorario, formado por vecinos copropietarios del complejo.

Explica que se trata de un medio de prensa de circulación interna y distribución gratuita dentro del complejo y que se financia a través de la comercialización de espacios publicitarios. Agrega que esa circulación interna cuenta con la autorización expresa de la Asamblea Central de Gobierno y Administración.

Agrega que efectivamente, en una de las secciones del periódico se informa sobre los temas que son tratados en el seno de esa Asamblea. Estas reuniones son de carácter abierto y los temas se difunden con anticipación entre las 61 Torres y entre los comerciantes. En razón de ello, BB alega que toda la información que publica es conocida por la totalidad de la población del complejo. Agrega además que todos los firmantes de la nota son funcionarios del complejo y por ello se los ha mencionado cuando se hace alusión a temas tratados en esas reuniones. En el caso de AA, que es mencionada en varias oportunidades, ello se debe a que es la contadora, o sea quien debe realizar varios trámites relacionados con la administración del edificio.

BB adjunta los ejemplares posteriores al 15 de junio de 2011, fecha en la que recibe la nota de los interesados en que sus datos no se sigan mencionando.

-III- Marco jurídico de la denuncia

La denuncia refiere a un hecho que podría estar alcanzado por las disposiciones vigentes en materia de protección de datos personales, debido a lo establecido en el artículo 4° literal d) de la Ley N° 18.331, que define al dato personal como “información de cualquier tipo referido a personas físicas o jurídicas determinadas o determinables”.

Sin embargo, la utilización de los nombres y demás información relacionada con estas personas, debe ser analizada en el contexto en el cual se desarrolla y en relación con los demás derechos que entran en juego.

En razón de lo expuesto es posible arribar a las siguientes consideraciones:

1. La Protección de Datos Personales es un derecho humano pero ello no significa que sea absoluto y no deba ceder ante la prevalencia de otros derechos y libertades constitucionalmente reconocidos y protegidos como lo son la libertad de información y de expresión, siempre que éstas se ejerzan dentro de ciertos límites. Por ello la veracidad, la finalidad y el interés general deben ser ponderados ante cada caso concreto.

2. El periódico “ZZ” se trata de una publicación y como tal, según lo expresa su Editor Responsable, ha sido inscripta en el registro del MEC. En este sentido deben ser ponderados también los derechos y libertades antes mencionadas.

3. Por otra parte, cuando se trata de un medio de información o de una publicación (por más pequeño alcance que ésta tenga), el tenor de la información que se publica nunca podrá ser enteramente objetiva, porque en definitiva refleja la opinión o la posición del grupo de personas responsables de su contenido. Por ello no es enteramente posible exigir a esta publicación independiente, que tiene fines informativos y comerciales, que sólo publique información objetiva o que no publique ciertos nombres.

4. Es importante tener en cuenta que la Ley N° 18.331, en su artículo 9° establece que el tratamiento de datos es lícito cuando el titular hubiere prestado su consentimiento o, en su defecto, cuando los datos provienen de fuentes accesibles al público o bien que existe una Ley que ampara ese tratamiento o una relación contractual o comercial entre el titular de los datos y el responsable del tratamiento. En el caso, se informa sobre temas que son tratados

en una asamblea abierta a todos los vecinos. Los nombres que se tratan son los nombres de los empleados del complejo, o sea que existe un vínculo contractual que habilita a que esos nombres se manejen asociados a los asuntos de su competencia. También existen leyes que amparan la libertad de prensa en nuestro país.

5. En definitiva, cuando “ZZ” informa sobre temas vinculados al complejo, -que además previamente ya han sido tratados públicamente en asambleas abiertas-, y a ello asocia el nombre de los empleados en principio no se estaría vulnerando la Ley, siempre que los demás datos asociados sean adecuados y no desproporcionados o excesivos con relación a esta finalidad. Si se reproduce el contenido de las actas de asamblea y éstas ya han sido divulgadas, tampoco cabría considerar que se ha vulnerado la Ley.

6. En este sentido, leída la información contenida en varios de esos periódicos, no se identifica cuál es la información de carácter personal que no debería ser publicada porque vulnera la integridad y sensibilidad de los denunciantes. Tampoco surgen datos que podrían considerarse excesivos o desproporcionados de acuerdo con la finalidad que poseen las publicaciones.

7. Corresponde aclarar a su vez, que si de la información que se publica en “ZZ”, surgen agravios, injurias u acusaciones relativas a los denunciantes, que significan para éstos un ataque personal, deberían realizar la correspondiente denuncia ante la justicia. Esta hipótesis no es de competencia de la URCDP.

Por lo expuesto cabe concluir que no estaríamos, en principio, ante un tratamiento de datos personales que vulnera la Ley N° 18.331.

Se solicita dar vista previa de este informe a los denunciantes, en los términos del art. 75 del Decreto N° 500/991, de 27 de setiembre de 1991.

Fdo. Dra. Graciela Romero
Derechos Ciudadanos

Informe N° 362, de 21 de agosto de 2012.

Se informa consulta de la Asesoría Letrada de la Dirección General de Registro sobre la publicación en la página web de las Resoluciones Administrativas.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|-------------------|
| 362 | 12 | 2012-2-10-0000560 |

Montevideo, 21 de agosto de 2012.

Ref. Consulta de la Dirección General de Registros.

-I- Introducción

Con fecha 28 de junio del corriente, la Asesoría Letrada de la Dirección General de Registro (DGR), consulta a la URCDP sobre la publicación en la página web de las resoluciones administrativas.

Según lo indicado la DGR consulta si puede publicar en su página web las resoluciones administrativas derivadas de peticiones o derivadas de contenciosos administrativos.

Las resoluciones son publicadas en forma íntegra, incluyendo nombres y “demás datos que sea del caso incluir en el texto de la resolución”. La finalidad de la publicación es dar a conocer la posición de la DGR en las diferentes materias.

Finalmente se indica que el objeto de la consulta es “saber si no se está de este modo violando los derechos de los usuarios al publicar la gestión realizada y sus datos personales, cuando en principio fueron aportados y recolectados para otros fines, como ser dar curso a la petición”.

-II- Análisis del marco jurídico

I) La URCDP está facultada a asesorar sobre el alcance de la Ley citada, de acuerdo a lo establecido en el art. 34. La presente consulta cuenta con elementos que fueron considerados por la URCDP con anterioridad.

II) Así el Dictamen N° 22/10 de 23 de setiembre de 2010, sobre una consulta de la Administración Nacional de Educación Pública, la URCDP establece que los registros públicos quedan por fuera del ámbito objetivo de la Ley N° 18.331.

III) La Dirección Nacional de Registros cuenta con una ley especial de creación y regulación, la Ley N° 16.871, por lo que entra dentro de la excepción planteada en al literal C) de la Ley N° 18.331.

IV) Respecto al consentimiento previo e informado que establecen los artículos N° 9° y 17, no es necesario recabar si los datos provienen de fuentes públicas tales como registros públicos.

-III- Conclusiones

Los registros públicos de la DGR quedan fuera del ámbito de aplicación de la Ley N° 18.331. No obstante lo anterior, los datos personales deben ser tratados de acuerdo a los principios generales de la protección de datos personales, a fin de resolver la mejor manera de publicar la información.

Se sugiere a la DGR el confeccionar versiones públicas de las resoluciones accesibles en su página web, mediante la disociación de los datos personales de los usuarios.

Fdo. Dra. Rosario Ierardo

Derechos Ciudadanos

Informe N° 430, de 23 de agosto de 2012.

Se informa consulta presentada por la Asociación de Despachantes de Aduana del Uruguay (ADAU) sobre datos publicados por la Dirección Nacional de Aduanas.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|------------------|
| 430 | 12 | 2011/05007/21529 |

Montevideo, 23 de agosto de 2012.

Ref. Consulta de la Asociación de Despachantes de Aduana del Uruguay

- I- Alcance de la consulta

Previo a Dictaminar en el Expediente de referencia (Consulta realizada por la Asociación de Despachantes de Aduana (en adelante ADAU), la Dirección de Asuntos Jurídicos y Notariales de la Dirección Nacional de Aduanas (en adelante DNA) solicita que AGESIC, -en el marco de las competencias otorgadas por la Ley N° 18.381, de 17 de octubre de 2010 según surge a fs. 17-, asesore acerca del carácter de confidencialidad que eventualmente poseen determinados datos personales de firmas pertenecientes a despachantes de aduana (empresas), cuyo acceso actualmente está permitido a terceros a través del Sistema Lucía.

Secretaría General de AGESIC a su vez, remite las actuaciones a la Unidad Reguladora y de Control de Datos Personales (URCDP) a efectos de que se pronuncie al respecto.

En definitiva, se requiere un pronunciamiento de la URCDP a efectos de fijar criterios que permitan publicar y/o acceder a los datos de las empresas, en este caso firmas aduaneras (DUA y Sistema de Datos Lucía), sin vulnerar el derecho a la protección de datos personales.

- II- La situación actual

Según la consulta realizada, el Decreto N° 333/992 ordena a la Aduana instrumentar un servicio de información disponible a consulta de los interesados (empresas vinculadas a estas actividades), que previamente haya gestionado la clave de acceso.

Mediante Resolución de 31 de diciembre de 2007, la Dirección Nacional de Aduanas resuelve poner en conocimiento de cada usuario el “Reglamento de Uso de Claves de Usuario y Acceso a Información” y mantener un archivo al día con las copias firmadas por los usuarios de dicho Reglamento.

La clave otorgada es personal e intransferible, está prohibido el otorgamiento de usuarios y claves colectivas, los usuarios ya existentes deberán haber firmado el Reglamento de Uso, así como a aquéllos que se lo requieran, previo otorgamiento de su clave (<http://www.aduanas.gub.uy/innovaportal/file/2158/1/od-2007-092.pdf>)

La ADAU, respecto a lo establecido en el Decreto 333/992, indica que dicha disposición no es genérica, sino que refiere a la publicación de determinados datos: número de despacho, codificación de la mercadería, descripción comercial, unidad de medida, volumen físico, valor unitario y total, países de origen y procedencia.

Agregan que en la actualidad, la información que se presenta en la web, -cuyo acceso se concede a todas las empresas registradas, incluyendo empresas que sistematizan y comercializan con dicha información-, contiene datos que exceden lo expresado en el decreto. Por ejemplo: se indica la identidad del titular de cada operación (importador, exportador, transitario), la identidad del despachante, así como del transportista.

En razón de ello entienden que, limitando la publicación sólo a los datos señalados en el mismo, sin asociárselos a la identidad de los intervinientes en cada operación, cuestión que no se indica en el decreto, se estaría garantizando el derecho a la protección de datos de las personas jurídicas.

Por su parte, la Dirección Nacional de Aduanas en su informe de 30 de mayo de 2012 aclara que surgen dos vías de acceso a la información de aduanas. Una es la de un sitio web de libre acceso: ftp. aduanas, que brinda todos los datos de las operaciones de comercio exterior que se realizan ante la Aduana de forma cruda y sin procesar, para lo cual requiere luego de un procedimiento informático específico.

La segunda forma es a través de las consultas web de los usuarios externos al Sistema Lucía que cuentan con clave de usuario, entre ellos se encuentran los Agentes Privados de Interés Público, así como las empresas y demás actores que justifiquen estar vinculados con las operaciones de comercio exterior que se tramitan ante la Aduana.

En la primera de las formas descriptas no se identifican riesgos para la protección de datos de las personas jurídicas, debido al carácter que poseen los datos que ahí se publican (en general tablas con metadatos, datos disociados o con el nombre de las empresas pero sin detalles en las cifras que se mencionan). El problema se presenta con la segunda opción.

La Dirección Nacional de Aduanas indica a su vez que, el alcance de ambos acceso ha sido delimitado, tal como se indica en el Informe de Referencia N° 6, a los datos del RUT y nombre de despachante y a los del DUA que incluyen: nombre y RUT del importador, datos de la mercadería (declaración arancelaria, valor, cantidad, ajustes, descripción comercial, origen, procedencia), tributos a pagar, pagados, documentos, certificados asociados al DUA (emitidos por otros organismos que intervienen en la operación de comercio exterior, como ministerios, LATU, licencias, certificados de origen, transportista, datos del contenedor). Los únicos datos que han dejado de publicarse son los datos del comprador y proveedor de la mercadería, los del remitente y destinatario (subrayado nuestro).

- III- Marco normativo que debe ser considerado

Para realizar este análisis corresponde considerar lo establecido en diversas normas que, -además de tener mayor jerarquía por ser leyes-, incluso han sido aprobadas en el último tiempo, como es el caso de la Ley de Protección de Datos Personales y Acción de Habeas Data.

En este sentido comenzaremos con lo expresado en el art. 13 de la Ley N° 17.243 "Las empresas que desarrollen actividades económicas, cualquiera fuere su naturaleza jurídica, están sujetas a las reglas de la competencia, sin perjuicio de las limitaciones que se establecieron por ley

y por razones de interés general (artículos 7º y 36 de la Constitución de la República) o que resulten del carácter de servicio público de la actividad de que se trate” (subrayado nuestro). En este sentido, si bien la Ley N° 18.381 de Acceso a la Información Pública, de 17 de octubre de 2008, refiere a las obligaciones de transparencia que deben garantizar las entidades públicas, en todos los casos donde se deben publicar o difundir datos personales, tanto de particulares como de empresas, - es necesario procurar un balance o equilibrio con el derecho a la Protección de los Datos Personales establecido en la Ley N° 18.331, de 11 de agosto de 2008.

A su vez, según el art. 10 de la Ley N° 18.381, no deben publicarse los datos personales que requieren previo consentimiento informado por constituir información confidencial.

Por otra parte, de acuerdo con el art. 9º de la Ley N° 18.331 no se requiere el consentimiento en los casos que allí se mencionan. En estos casos, cuando se está actuando en el ámbito de las excepciones previstas en los literales b) y d) del artículo 9º de la Ley N° 18.331, la información que contenga datos personales, debe recabarse (la Ley N° 18.331 no dice publicar, difundir o comunicar) para cumplir con las funciones propias del organismo o ser necesarios para el desarrollo de una relación contractual, científica o profesional.

En definitiva es correcto considerar que, si se toma en cuenta el principio de finalidad, -establecido en el artículo 8º de la Ley N° 18.331-, al publicar esos datos en forma íntegra se estarían empleando con un fin distinto o excediendo el ámbito donde funcionan las excepciones, porque se va mas allá del consentimiento genérico otorgado en virtud de la relación comercial o del ejercicio de las funciones propias de los poderes del Estado.

La publicación en la web de determinados datos personales, -aún actuando dentro de las excepciones-, en definitiva implica una comunicación de los mismos según lo establece el art. 17, por ende para publicar toda la información, sin limitarse exclusivamente al elenco de datos que se mencionan en el Decreto 333/992, habría que practicar un procedimiento de disociación de la información de modo que los titulares o intervinientes no fueran identificables.

De lo contrario, sólo podrían publicarse aquellos datos que no requieren previo consentimiento informado, que en el caso de las personas jurídicas son: razón social, nombre de fantasía, RUT, domicilio, teléfono e identidad de las personas a cargo de la misma, obviando toda la información comercial.

- IV- Sobre los datos personales de las personas jurídicas

Como ya se ha expresado, según lo establecido en el art. 9º, existen determinados datos personales que no requieren para su tratamiento el previo consentimiento del titular. Por otra parte, el literal b) del artículo 9º establece que no es 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 ese sentido, tomando en consideración los cometidos inherentes a la Aduana y su marco legal, cabe inferir que no se debe recabar el consentimiento de dichas empresas a efectos de cumplir con sus funciones o cometidos, así como para comunicar esos datos a determinados

organismos públicos (Ministerio de Economía, por ejemplo), cuando ello corresponde atendiendo a las funciones o cometidos de cada uno, a la finalidad del intercambio y a la regulación legal de dicho funcionamiento²⁹.

Además, de acuerdo con la Ley N° 18.331 hay 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.

De igual forma corresponde considerar que, lo anterior de ningún modo habilita a brindar acceso a terceros de todos los datos que pertenecen a estas empresas: sus clientes, volumen comercial, cantidades de operaciones que realiza, su productividad, etc., porque para la publicación de estos datos debe atenderse a lo establecido en el art. 2 de la Ley, en lo referente a la extensión del derecho a la protección de datos personales a las personas jurídicas, en cuanto corresponda.

Esto también se relaciona en forma directa con el derecho que poseen las empresas al resguardo de parte de su información ante la competencia, buscando evitar la competencia desleal, proteger una serie de conocimientos técnicos que poseen valor comercial y son desarrollados por ellas y que en definitiva pueden ser útiles para sus competidores.

Justamente, la Ley N° 18.381 de Acceso a la Información Pública establece que debe ser clasificada como confidencial la información entregada por los particulares en tal carácter a los sujetos obligados, siempre que:

- Refiera al patrimonio de una persona física o jurídica.
- Comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica, que pudiera ser útil para un competidor.
- Esté amparada por una cláusula contractual de confidencialidad.

También se considera información confidencial, a los datos personales que requieran previo consentimiento informado, tal como se establece en la Ley N° 18.331 de Protección de Datos Personales. Determina a su vez que tendrán el mismo carácter los documentos o secciones de documentos que contengan estos datos.

Esto indica que se reconoce a las empresas la posibilidad de proteger cierta información que les pertenece: ya sea cuando la presentan ante la Aduana (o ante cualquier sujeto obligado), en aquellos casos que refiera a alguna de las hipótesis previstas en la norma. En este sentido se pueden señalar o identificar los documentos o secciones que contengan dicha información confidencial y el organismo debe tratarla como tal. Se entiende por tanto que la información declarada confidencial, no podrá ser puesta en conocimiento de otras partes dentro de un procedimiento, ni divulgada a terceros. Los despachantes entonces perfectamente podrían solicitar que se considere confidencial, parte de la información que entregan a la Aduana.

²⁹ *Respecto al intercambio de información entre organismos públicos, estatales o no, se debe estar a lo dispuesto en los arts. 157 a 160 de la Ley N° 18. 719 de 27 de diciembre de 2010.*

Lo anterior indica a su vez, una voluntad jurídica dirigida a proteger determinada información de las empresas, lo cual se suma a lo ya expresado respecto a la extensión del derecho a la protección de datos personales a las personas jurídicas, incluido en el art. 2 de la Ley N° 18.331.

La URCDP ya se ha pronunciado en este sentido, en el Dictamen N° 1/009 recaído en la Consulta sobre Anteproyecto de Ley referido a Publicidad de Certificados que otorga el BPS³⁰. En este caso, ante la posibilidad de publicar ciertos datos, 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.

En el Dictamen N° 10, de 8 de julio de 2011 sobre consulta de la Dirección Nacional de Medio Ambiente referida a entregar o no información relativa a plantas industriales. La Unidad dictamina que ante la falta del consentimiento, procede la disociación de los datos referidos a los nombres de las empresas que presentaron los informes y que contienen los siguientes datos: nombre de la empresa, cantidad producida de todos los productos, consumo de agua, consumo de energía, personal empleado por turno, días trabajados, caudales de los efluentes líquidos, detalle de las muestras.

-V- Conclusión

Si bien la Dirección Nacional de Aduanas no está obligada a obtener el consentimiento para recabar los datos contenidos en el DUA o en otros documentos necesarios para dar trámite a las importaciones y exportaciones; así como tampoco para comunicarlos a determinados organismos públicos en el marco de sus competencias y funciones (Ministerios, LATU), sí debe atenderse a la confidencialidad que puede revestir cierta información comercial de las empresas, así como a la de aquellos datos personales que sí requieren el previo consentimiento a efectos de ser comunicados a terceros.

Fdo. Dra. Graciela Romero

Derechos ciudadanos

30

<http://www.datospersonales.gub.uy/sitio/dictamenes/2009/dictamen-1-009.pdf>

Informe N° 414, de 27 de agosto de 2012.

Se informa sobre consulta del Ministerio de Salud Pública, División Epidemiología, respecto a la aplicación de la ley N° 18.331 a las bases de datos relativas a la mortalidad, natalidad, información perinatal y enfermedades de notificación obligatoria.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|--------------------|
| 414 | 12 | 2012-02-10-0000668 |

Montevideo, 27 de agosto de 2012.

Ref. Consulta MSP, División Epidemiología.

I. Introducción.

La Dirección Epidemiología del Ministerio de Salud Pública formula consulta a la Unidad Reguladora y de Control de Datos Personales (URCDP), respecto a la aplicación de la Ley N° 18.331, de 11 de agosto de 2008, a las bases de datos relativas a la mortalidad, natalidad, información perinatal y enfermedades de notificación obligatoria de las cuales es responsable. Se consulta acerca de la aplicación de la ley a ciertas situaciones a las cuales se enfrenta la División en su labor diario.

En virtud de la consulta recibida y en cumplimiento de las facultades que le son otorgadas la URCDP por el artículo 34 de la Ley, la Unidad procede a la sustanciación de ésta.

II. Análisis de la consulta.

Se procederá al análisis individual de cada una de las preguntas formuladas.

II.a. A los fines de la ley, ¿cuáles se consideran “sucesores universales” (artículo 14)? En este caso, ¿cómo se acredita su condición a los fines de comunicar datos personales sensibles de un familiar fallecido? En el caso de terceros (no sucesores universales) debe presentarse poder que lo acredite, ¿es correcto? ¿Qué sucede en el caso de padres del titular de los datos? ¿Qué documentación se exige en esta última situación en caso de solicitar datos sensibles de un hijo de ser menor de edad? (en los mayores se solicitaría consentimiento o poder).

El artículo 14 de la ley N° 18.331 consagra el derecho de acceso de los titulares de datos personales. También prevé la posibilidad, en caso de personas fallecidas, de que los sucesores universales puedan ejercer el derecho de acceso siempre que acrediten debidamente esta calidad.

Se considera que debe analizarse cada caso concreto para determinar que se debe solicitar como elemento probatorio de tal situación. Puede presentarse el caso de que exista una sucesión finalizada y los herederos cuenten con el certificado de resultancia de autos que acredite su calidad. También podría considerarse válido un certificado notarial de presuntos herederos. Por otra parte, podría probarse tal calidad a través de los testimonios de partidas de registro de estado civil.

Es de resaltar que el artículo 32 del Decreto N° 274/010 de 8 de setiembre de 2010 también refiere al ejercicio del derecho de acceso en el mismo sentido que la ley de protección de datos personales, indicando que éste corresponderá a cualquiera de los sucesores universales debidamente acreditados.

En el caso de los terceros que pretendan obtener datos de personas fallecidas presentando poder, debe tenerse presente lo dispuesto en el inciso 5 del artículo 2068 del Código Civil el cual indica que el mandato se acaba “Por muerte del mandante o del mandatario”. Ello es aplicable en todos los casos, salvo lo dispuesto por el artículo 2096 del mismo cuerpo normativo: “No se extingue por la muerte del mandante el mandato destinado a ejecutarse después de ella”. Por lo expuesto, tratándose de personas fallecidas, salvo situaciones excepcionales, no podría presentarse un tercero que no posea la calidad de sucesor universal.

En la consulta referida a los representantes legales de los titulares de datos menores de edad se entiende que pueden ejercer el derecho de acceso respecto a los datos de sus representados, acreditando debidamente su condición. Por otra parte, debemos sumar las previsiones de la Ley N° 18.335, de 15 de agosto de 2008 y su decreto reglamentario N° 274/010 de 8 de setiembre de 2010 que se refieren a los derechos y deberes de los pacientes, referidas al tratamiento de los datos de salud de los niños, niñas y adolescentes, tanto referidas al consentimiento informado como a la confidencialidad de la historia clínica de los adolescentes, en las condiciones establecidas por la normativa mencionada.

II.b. ¿Existe algún mecanismo legalmente válido para la comunicación de datos personales sensibles a un tercero, distinto a la disociación o firma del consentimiento informado? Esta consulta refiere por ejemplo a las solicitudes de investigadores de datos personales correspondientes a enfermedades o defunciones que no son de utilidad si se disocian de su titular (por ejemplo para la búsqueda de pacientes asistidos por una patología para los que se intenta saber si fallecieron o no a causa de cierta patología).

La Ley N°18.331 establece que para la comunicación de datos personales se requiere, como principio, el previo consentimiento del titular de los datos regulado en su artículo 9°. Por su parte, el artículo 17 dispone las excepciones a este principio, fundamentalmente debemos tener presente el literal C) (en la redacción dada por el artículo 153 de la Ley N° 18.719), que refiriéndose a datos relativos a la salud indica que no será necesario el consentimiento cuando: “Se trate de datos personales relativos a la salud y sea necesaria su comunicación por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de los titulares de los datos mediante mecanismos de disociación adecuados cuando ello sea pertinente”.

Además de lo expuesto, el literal B) del mismo artículo al excepcionar el consentimiento, nos remite al artículo 9° de la ley. En este artículo merece comentar a éstos efectos, el literal B), que excepciona de consentimiento a aquellos datos que se recaben para el ejercicio de los poderes propios del Estado o en virtud de una obligación legal. En la consulta formulada se debe tener presente que la comunicación de datos sería legítima entre organismos del estado cuando la misma se realice en el sentido expresado por el artículo comentado.

Esta excepción reconoce su fuente en España, en la Ley N° 15/999, y a su respecto se ha dicho que “el tratamiento de los datos personales no precisará del consentimiento de los afectados cuando sea preciso para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias”. (Protección de Datos Personales para Administraciones Locales, APCM, pág. 151).

II.c. ¿Cómo se define quienes pueden ser considerados “encargados del tratamiento” de datos personales? Esta consulta refiere puntualmente a solicitudes de datos personales (no disociados) por otros sectores del MSP distintos a Epidemiología o vinculados al MSP (por ejemplo las Comisiones Honorarias, autoridades, etc.). Estos sectores pueden requerir para sus funciones el uso de datos personales (por ejemplo para realizar estimaciones de sobrevida), si bien el área responsable de dicho trabajo es la División Epidemiología. ¿Es posible considerar a estos también como “encargados del tratamiento” a pesar de no formar parte de la División? A su vez esta pregunta nos dirige a otra: ¿quién y cómo se define quiénes son “terceros” a los fines de la ley? ¿Cómo se establecen las personas “autorizadas para tratar los datos bajo la autoridad directa del responsable” según el artículo 4°?

Se debe tener presente que tratándose de comunicaciones de datos en el ámbito del Ministerio de Salud Pública, se aplican las previsiones mencionadas en el apartado anterior respecto a que no requiere consentimiento las comunicaciones de datos cuando éstos han sido recabados en virtud de las funciones propias del organismo o en virtud de una obligación legal. Cuando se trate de comunicaciones en el ámbito del Ministerio o entre sus diversas divisiones, para el cumplimiento de sus actividades, la comunicación de datos resultaría legítima.

En el caso de que se trate de comunicaciones de datos a otros organismos del estado, se deberá analizar en cada caso si corresponde la excepción referida en la pregunta anterior.

II.d. ¿Es legalmente válido comunicar datos personales sensibles solicitados por juzgados? ¿Es legalmente válido comunicar datos personales sensibles solicitados por abogados representantes de un tercero (distinto al titular al que se refiere el dato)?

En el caso de la solicitud de información a través de un mandato judicial, se entiende que es válida la entrega de ésta. Debe tenerse presente lo dispuesto por el artículo 30 del Decreto 274/010, de 8 de setiembre de 2010 que regula la reserva de la historia clínica y la restricción del acceso a ésta, estableciendo en su inciso final que los servicios de salud y sus trabajadores

deben mantener reserva respecto a la historia clínica salvo que su revelación sea necesaria para el tratamiento del paciente o mediante orden judicial.

No se considera adecuada la comunicación de datos a los abogados representantes de un tercero, en virtud de los elementos ya vertidos en el presente informe a propósito del consentimiento informado del titular de los datos personales.

II.e. En el caso concreto de que compañías aseguradoras soliciten copia del certificado de defunción de uno de sus asegurados, ¿es válida su entrega en caso de que estos presenten copia del consentimiento de la persona fallecida realizado durante la contratación del seguro? La respuesta a esta interrogante es afirmativa. La empresa que solicite el certificado de defunción deberá presentar el documento que acredite que el titular de los datos ha prestado su consentimiento en forma libre, expresa e informada de acuerdo a las exigencias del artículo 9° de la ley. Tratándose de contratos de seguro, en cualquiera de sus variantes, la obtención de la información se encuentra asociada a la finalidad perseguida por el asegurado al celebrar el contrato.

II.f. ¿Qué formato de consentimiento y/o poder es válido para la comunicación de datos personales sensibles?

Las condiciones que deben cumplirse para la comunicación de datos están referidas en el artículo 17 de la ley. Los datos pueden ser comunicados para el cumplimiento de los fines relacionados al interés legítimo del emisor y del destinatario, con el consentimiento expreso y escrito de su titular, al cual se debe informar sobre la finalidad de la comunicación e identificar al destinatario de los datos o proveerlo de elementos suficientes para su identificación.

En la página web de la URCDP se encuentran disponibles modelos de cláusulas de consentimiento informado a las cuales pueden agregarse el consentimiento para la comunicación de datos con las condiciones mencionadas. Dichas cláusulas pueden ser presentadas ante la Unidad para su consideración. Información disponible en: <http://www.datospersonales.gub.uy/sitio/destacados.aspx>.

II.g. ¿Es legalmente válida la publicación web de bases de datos personales sensibles si éstos están disociados? ¿Qué datos deben eliminarse en este caso para considerarse “disociados” según se explicita en el artículo 18?

Se considera que la publicación de datos en la web podría realizarse siempre que se cumpla con lo dispuesto en el literal D) del artículo 17 de la ley, respecto a los procedimientos de disociación de la información.

La disociación de datos personales se encuentra definida en el literal G) del artículo 4° de la ley como: “todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable”. El proceso de disociación implica que sea imposible asociar un dato con una persona determinada.

III. Conclusiones.

De la consulta planteada, surge el interés de la consultante en adecuar sus procedimientos a la normativa vigente en materia de protección de datos personales, la cual debe armonizarse, cuando corresponda, con las normas relativas a derechos y deberes de los usuarios de la salud.

Se recomienda que frente al planteamiento de situaciones dudosas, se tenga presente la naturaleza sensible de los datos de salud de cuyo tratamiento es responsable la consultante, y se tomen como rectores los principios en materia de protección de datos personales consagrados en el artículo 5° y siguientes de la Ley N° 18.331, con especial atención al principio de previo consentimiento informado.

Fdo. Dra. Jimena Hernández

Derechos Ciudadanos

Informe N° 428, de 4 de setiembre de 2012.

Se informa sobre Proyecto de Ley sobre censura previa y derecho de respuesta en redes sociales.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|--------------------|
| 428 | 12 | 2012-02-10-0000671 |

Montevideo, 4 de setiembre de 2012.

Ref. Análisis del Proyecto de Ley sobre prohibición de censura previa y derecho de respuesta en redes sociales.

I. El contenido del Proyecto de Ley

El mismo consta de una Exposición de Motivos y ocho (8) artículos.

En la Exposición de Motivos se comenta el crecimiento exponencial de Internet, y su influencia en la vida de las personas, el comercio, los países y la innovación. Se hace hincapié en un aspecto particular de este medio técnico como es el favorecimiento de la libertad de expresión, analizándose ésta a partir del art. 29 de la Carta y una exégesis histórica. Se sostiene que se debe equiparar la situación de las redes sociales a la de otros medios de comunicación, respetando los principios y derechos consagrados en el citado art. 29 (la no censura previa y responsabilidad a posterior del emisor) y en los arts. 7° y siguientes de la Ley N° 16.099 (derecho de respuesta). Se pugna por regular estos tópicos para adaptarlos a la nueva forma de comunicación.

El art. 1° declara que la protección de los derechos al honor y la intimidad (arts. 7° y 72 de la Carta), comprende la afectación de estos derechos por medio de redes informáticas.

El art. 2° prohíbe la censura previa de las redes informáticas, sin perjuicio de la responsabilidad del autor a posteriori y con remisión al art. 29 de la Carta.

El art. 3° consagra una acción judicial de restricción o bloqueo de acceso a contenidos lesivos, remitiendo a la competencia y procedimientos de la Ley N° 16.011 (Ley de Amparo), con facultades incluso cautelares.

El art. 4° confiere legitimación procesal de estas acciones al Ministerio Público, tratándose de incapaces y menores edad, sumándose a la de sus representantes legales. El inciso segundo aclara que el artículo será de aplicación en particular a los casos de exhibición pornográfica.

El art. 5° reconoce el derecho de rectificación y respuesta, a ejercitar en relación a la actividad desarrollada a través de estos medios cuando se estuviera frente a una información expuesta en términos agraviantes, disminutorios o capaces de producir rechazo social. Se

hacen remisiones expresas a los arts. 15 y 16 de la Ley N° 18.331 (derecho de rectificación, actualización, inclusión o supresión, y derecho a la impugnación de valoraciones personales, todo ello con relación a datos personales), y en los arts. 7° y 12 de la Ley N° 16.099 (derecho de respuesta en materia de libertad de comunicación de pensamientos y libertad de información).

El art. 6° estipula que el derecho de respuesta regulado en el Capítulo III de la Ley N° 16.099 es aplicable a los proveedores de redes informáticas, motores de búsqueda, portales y similares, existentes en sitios web bajo código de nuestro país, por el lapso de hasta un año contabilizado desde la presencia en la red de la información que lo origina.

El art. 7° obliga a los proveedores de redes informáticas y motores de búsqueda presentes en sitios web bajo código de nuestro país, a agregar una dirección de correo electrónico para atención de consumidores o usuarios, con la obligación -además- de confirmación automática de los mensajes.

El art. 8° remite al precepto constitucional de inviolabilidad contenido en el art. 28 de la Carta, a los paquetes de contenido, correos electrónicos y demás correspondencia que circula en la red.

II. Comentario general

La mayoría del articulado propuesto, no se comparte. En algunos casos por razones de forma pero -sobre todo- por razones sustanciales.

Lo sustancial para emitir este juicio negativo es que se parte de premisas de razonamiento a nuestro juicio equivocadas, a saber:

A) La necesidad de introducir nuevas previsiones con fuerza de ley en un campo tan delicado como es el ejercicio de derechos y valores fundamentales, en este caso para atender el escenario planteado por las redes sociales que -para colmo- no se las nombra a texto expreso más que en el título y la exposición de motivos, creando confusión al respecto (“redes sociales” es una cosa, “redes informáticas” como rezan todas las entradas del articulado proyectado, es otra).

B) La liviana equiparación de las nuevas formas de comunicación electrónica al régimen jurídico de la prensa, cuando una asimilación completa no es posible, en tanto no exista un productor o editor fácilmente ubicable a quien llamar a responsabilidad.

No se ha advertido que la libertad de expresión y su posible ponderación o limitación cuando existen abusos, nunca ha sido tema de fácil abordaje para el legislador en ninguna época y lugar, por más que exista la segunda frase del art. 7° de la Constitución.

De esta dificultad ínsita debe extraerse una clara enseñanza: mínimos intervencionismos legislativos, reservados para casos claros y excepcionales. Y dejar que sean los jueces la mayoría de las veces quienes -en definitiva- se encarguen de ejercitar con propiedad la delicada

labor de ponderación y amparo de ésta tan preciada libertad, en un complejo escenario de balances y contrabalances entre múltiples valores en juego, cuya correcta elucidación no es campo apropiado para cerrarlo esquemáticamente mediante leyes especiales.

En materia de libertad de comunicación de pensamientos la normativa general existente debe considerarse suficiente. O en todo caso, si hubiera que reformarla, ello no debería ocurrir al influjo de las nuevas formas de información y comunicación puesto que nunca ha ocurrido antes tampoco con otras tecnologías supervinientes al tradicional medio escrito. No se conocen leyes que digan que el mensaje de radio, televisión, etc. no puede afectar el honor y la intimidad, ni que se prohíba la censura previa en estos medios en particular. Menos aún que quepan acciones judiciales cautelares o de fondo especialmente concebidas para un medio de comunicación.

Habrà de tenerse presente, sobre todo, la innecesariedad de dictar nuevas leyes cuando lo dispuesto por el art. 1º de la Ley Nº 16.099 es de tal amplitud que no deja lugar a duda alguna en cuanto a la inclusión de toda forma de expresión, incluyendo las que provengan de lo que el proyecto normativo denomina “redes informáticas” (que poco y nada se sabe a qué refiere concretamente, como se dijo antes): “Artículo 1º (Libertad de comunicación de pensamientos y libertad de información).- Es enteramente libre en toda materia, la expresión y comunicación de pensamientos u opiniones y la difusión de informaciones mediante la palabra, el escrito o la imagen, por cualquier medio de comunicación, dentro de los límites consagrados por la Constitución de la República y la ley.”

Actualmente se debe tener presente, asimismo, que la enunciada amplitud se ha visto reforzada por lo dispuesto por el art. 3º de la Ley Nº 18.515, de 26-06-2009, que vino a incorporar el siguiente texto al inciso final del Art. 1º de la Ley Nº 16.099:

“Constituyen principios rectores para la interpretación, aplicación e integración de las normas civiles, procesales y penales sobre expresión, opinión y difusión, relativas a comunicaciones e informaciones, las disposiciones consagradas en la Declaración Universal de Derechos Humanos, en la Convención Americana sobre Derechos Humanos y en el Pacto Internacional de Derechos Civiles y Políticos. Asimismo, se tomarán en cuenta muy especialmente los criterios recogidos en las sentencias y opiniones consultivas de la Corte Americana de Derechos Humanos y en las resoluciones e informes de la Comisión Interamericana de Derechos Humanos, siempre que ello no implique disminuir los estándares de protección establecidos en la legislación nacional o reconocidos por la jurisprudencia nacional”.

En suma, no se advierte la necesidad de crear nuevos cuerpos legales al influjo de la aparición sucesiva de tecnologías en este punto, cuando ya se cuenta con el art. 29 de la Carta, con la Ley Nº 16.099 de 03-11-1989 en frecuente revisión y actualización, y con un Capítulo VI del Libro II del Código Penal, arts. 333 a 339 (Delitos de Difamación e Injurias), conformando una suma de dispositivos jurídicos de alcance general pero suficiente por lo abarcativo, en el que ingresa sin mayores problemas el uso eventualmente desmedido de las redes informáticas (vg. redes sociales).

III – Comentario de los artículos propuestos

El Art. 1º no es compatible por cuanto el hecho de declarar que la protección de ciertos derechos constitucionales abarca su afectación por medio del empleo de las redes informáticas, equivale que declarar que lo que se exprese en la vía pública o a través de algún medio de comunicación tradicional (prensa, radio...) afecta tales derechos. Son conductas que ya están reflejadas en la normativa existente. Resulta sobreabundante, y por ende innecesario, volver a legislar al respecto.

El Art. 2º y el Art. 3º son rechazables por las mismas razones que las apuntadas, a las que se agregan en el segundo caso las siguientes: a) la restricción o bloqueo de direcciones telemáticas ya ha sido aceptada por nuestros tribunales en atención a otro tipo de fundamentos, sin necesidad de dictar leyes con previsiones especiales al respecto; b) el “proceso cautelar” y el “proceso de amparo” están legislados de modo suficiente para contemplar todo tipo de situaciones, por lo que no es de buena técnica legislativa seguir agregando remisiones o supuestas adaptaciones cuando no existe necesidad para ello.

Con respecto al Art. 4º es del caso advertir que no se aprecia el motivo de dictar una nueva ley para tener por vigente la intervención del Ministerio Público en este tipo de asuntos como en cualquier otro, cuando resulten afectados intereses de menores e incapaces. De hecho el Ministerio Público tiene atribuidos deberes y poderes enderezados a la defensa menores e incapaces en cualquier ámbito, a través del Dec. Ley Nº 15.365, de 30-12-1982 (Ley Orgánica del Ministerio Público y Fiscal), en particular su art. 10 inc. 5º: “Actuar en todos los asuntos relativos a las personas e intereses de los menores, incapaces y ausentes, incumbiéndole en ese concepto los deberes que la ley le señale, y, expresamente, aquellos que derivan de la condición de protector oficial de los menores e incapaces que esta disposición consagra.”

Nos parece totalmente inadecuado extender el derecho de rectificación y el derecho de respuesta a las redes sociales según lo expresan el Art. 5º y el Art. 6º del Proyecto de Ley en examen. Hacerlo así implicaría asumir otro tipo de forzosas consecuencias de muy dudosa aceptación en el estado actual del Derecho como disciplina científica. Nos referimos a consideraciones ya apuntadas en otra parte del Informe, en cuanto a considerar el espacio de las comunicaciones telemáticas globales y abiertas en términos equivalentes a los de un medio masivo de comunicación de tipo periodístico, que no lo es. Somos de la idea que este tipo de asimilaciones resultan jurídicamente incorrectas, y conducen a sostener escenarios improcedentes e inviables, como el de suponer que a cada mensaje volcado en espacios web que resulte conflictivo con un DD.HH. se abra una instancia de derecho de respuesta, responsabilidad del editor, etc. El mundo virtual como el real, están sujetos en este punto a la misma normativa constitucional y civil en materia de DD.HH., limitaciones, responsabilidades, etc. Tanto la Ley Nº 16.099 como la Ley Nº 18.331 poseen un conjunto de definiciones y campos de aplicación satisfactorios y auto suficientes, sin necesidad de otra ley que venga a agregar nueva regulación e integrar fenómenos no siempre integrables.

Otra muestra de innecesaria duplicación de leyes surge del Art. 7º. Poniendo por caso que estemos ante un proveedor de red o motor de búsqueda nacional (mínima parte seguramente de lo que acontece en el ciberespacio sin fronteras), el mismo ya está alcanzado por la normativa internacional y nacional sobre direcciones IP y nombres de dominio, como también le resulta aplicable la normativa que regula a los proveedores en las relaciones de consumo (art. 3º Ley N° 17.250). No es necesario seguir dictando leyes al efecto.

Igual defecto de repetición innecesaria se aplica al Art. 8º, en tanto nadie ha puesto en tela de juicio que los correos electrónicos son una forma de correspondencia, como tal amparada por el art. 28 de la Carta.

IV. Conclusiones

El proyecto de ley en examen nos merece un juicio desfavorable. Hay debates que no se han dado en el país y quizás tampoco suficientemente en el campo doctrinario del Derecho aplicable a las TI. No sería buena cosa que vinieran a zanjarse o congelarse posiciones dictándose leyes de este tipo, sin previa valoración de todo lo que está en juego. Un ejemplo: El derecho de respuesta está previsto para las publicaciones ofensivas realizadas en “medios de comunicación pública” (art. 7º de la Ley N° 16.099). ¿Son las redes sociales una especie de ellos? Nuestra respuesta es que no lo son. No se puede identificar un medio de comunicación electrónica con un mass media por sí solo. Si un periódico de tiraje masivo tiene su canal de expresión a través de Internet, lo será. Pero si un señor protestón decide levantar su tribuna personal contestataria a través de su blog, no por eso se convertirá en un mass media al que se le aplique automáticamente el comúnmente denominado “derecho de la prensa” en toda su extensión. No se debe confundir el canal con el contenido. Es de alto riesgo y consecuencias hacerlo. Uno de estos riesgos o consecuencias de adoptar premisas de tal tipo es la de considerar “fuente pública de información” todo lo que habita en el ciberespacio sin restricciones de acceso. ¿Alguien está dispuesto a dar ese paso? Nosotros no lo estamos. Por este tipo de consideraciones, y por prever en la mayoría de su articulado cuestiones que ya están resueltas en otras normas, no compartimos la filosofía y el texto del Proyecto de Ley examinado.

Fdo. Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 481, de 12 de setiembre de 2012.

Se informa sobre consulta Proyecto de Ley presentado por los Senadores Francisco Gallinal y Luis Alberto Lacalle en relación con la modificación del art. 22 de la Ley N° 18.331.

| INFORME No. | | EXPEDIENTE No. |
|-------------|----|--------------------|
| 481 | 12 | 2012-02-10-0000670 |

Montevideo, 12 de setiembre de 2012.

Ref. Proyecto de Ley que modifica art. 22 de la Ley.

I. Encuadre general

El Proyecto de Ley consta de una Exposición de Motivos y seis artículos.

En la Exposición de Motivos se resalta la dimensión y gravitación que han ganado las bases de datos de consulta pública en la vida económica, las que deben contemplar la defensa de los derechos de todas las partes involucradas: acreedores, deudores y terceros consultantes. Se reconoce el alto impacto que tiene en la sociedad el registro de deudas económicas de personas físicas, limitando muchas veces el desempeño económico y provocando mayores perjuicios, incluso, que un embargo pronunciado judicialmente e inscripto en el correspondiente registro estatal (Registro Público de Embargos e Inhibiciones), el cual no proporciona información a terceros con las características que lo hacen los “clearings” privados, por ejemplo manteniendo el registro de operaciones cumplidas.

Se explican los alcances del Proyecto y su referencia exclusiva a las personas físicas por considerar que no se asimilan en su situación a las personas jurídicas. Se regula un procedimiento de notificación y descargos previo a registrar los adeudos, justificando la exclusión de aquellas hipótesis referidas a obligaciones sancionatorias o por incumplimientos de tasas o servicios en la medida que el Estado dispone de poderes revisables en vía jurisdiccional.

El Proyecto aboga, según reza, por “establecer exigencias, condiciones y límites que protejan al que actúa de buena fe y cumple con sus obligaciones.”

- II - Análisis del texto propuesto

El artículo 1° consagra la obligación de notificar a los deudores personas físicas la inscripción en registros privados de morosos con acceso a terceros, por parte de acreedores privados y públicos, con requisitos de plazo y contenido al efecto.

Se trata de una norma garantista, que le permite al afectado tomar conocimiento de la causa y oportunidad en la que un acreedor resuelve informar la situación a alguna base de datos de titularidad física o jurídica (quedan excluidos los registros públicos).

Se comparte el criterio y sentido de la norma. Sin desmedro de ello, a juicio del suscrito el beneficio de esta garantía debería extenderse a los deudores personas jurídicas. No vemos inconveniente en ello, máxime cuando nuestro legislador ha estado conteste en hacerlas parte del régimen general (art. 2° de la Ley N° 18.331), por lo que resultaría un elemento disonante

y discriminante dejarlas a un lado según es postura del Proyecto normativo en examen. Por iguales razones de coherencia y eliminación de todo factor de distorsión o discriminación del régimen de protección de datos personales en su conjunto, entendemos necesario ampliar el alcance de este Proyecto normativo a las bases de datos de pertenencia pública con acceso a terceros, como la CRC del Banco Central del Uruguay.

El artículo 2º regula un procedimiento destinado a recibir y tramitar los eventuales descargos del deudor cuya obligación incumplida es objeto de registro. Estamos ante una previsión igualmente loable además de consecuencialmente lógica con lo dispuesto en el artículo 1º, desde el momento que si se prevé una notificación al afectado no es para otra cosa que para darle la posibilidad de alguna suerte de ejercicio de derechos de defensa frente a la pretensión registral del acreedor.

Existiendo objeciones o descargos del afectado, la norma contempla opciones para el responsable de la base de datos cuya bondad técnica también reconocemos:

1º- Rechazar la inscripción hasta que el tema se resuelva en la esfera correspondiente.

2º- Efectuar la inscripción con una advertencia destinada a terceros que buscan información relativa al deudor involucrado, de que en este caso se trata de una información objetada.

La extensión del régimen sancionatorio contenido en el art. 35 de la Ley Nº 18.331 es también compartible. Sin perjuicio de ello se señalan dos defectos de redacción que conspiran contra el correcto entendimiento de la norma:

1º – El art. 35 de la Ley Nº 18.331 fue modificado, por lo que el texto de remisión empleado no parece suficiente. Para solucionar este aspecto no basta agregar “...en la redacción dada por el art. 152 de la Ley Nº 18.719” porque no quedarían a resguardo futuras modificaciones. Tampoco sirve la alternativa “... y posteriores que se dicten” porque se trataría de una norma sancionatoria en blanco que no está permitido. En estos casos, la mejor solución a juicio del suscrito sería una remisión genérica a “las disposiciones de la Ley Nº 18.331, modificativas y concordantes”.

2º – La alusión al “obligado” en el inciso 2º del artículo no es correcta y confunde, debiéndose sustituir la expresión por la de “acreedor”.

El artículo 3º permite prescindir de la notificación regulada en los artículos precedentes, cuando se está ante obligaciones reconocidas de modo firme en vía judicial o arbitral, solución natural y compartible que no merece mayor comentario por ello.

El artículo 4º propone un texto sustitutivo del inciso segundo del art. 22 de la Ley Nº 18.331 (datos relativos a la actividad comercial o crediticia), abatiendo los plazos registrales que pasarían de 5 + 5 en el régimen vigente, a 3 + 2 en el propuesto. Asimismo se deroga el registro de obligaciones canceladas o extinguidas, mediante norma prohibitiva.

Ambos aspectos fueron estudiados por la Unidad con detención en oportunidad de tratar el Proyecto de Ley del Arq. Aldo Lamorte (Exp. Nº 2847 del año 2010, Informe Nº 2540-2010 y Resolución Nº 1356-2010).

Cuando nos tocó informar al respecto (Informe 2540-2010) sostuvimos la bondad de ambas soluciones, sin perjuicio de la postura dictaminante de la Unidad respecto del abatimiento de plazos registrales también propuesto en el Proyecto Lamorte (3 + 3 en este caso), haciendo la salvedad de “que existen aspectos atinentes al funcionamiento del mercado económico, cuya consideración no compete, estrictamente a esta Unidad” (Res. 1356-2010).

El artículo 5º reformula el inciso cuarto del ya citado art. 22 de la Ley Nº 18.331 ajustando la redacción anterior y dando una versión consecuente con la prohibición de registrar datos comerciales positivos contenida en el artículo 4º del mismo Proyecto. La apelación al concepto de “obligación extinguida” en vez de “obligación cancelada” que figura en el texto original vigente resulta compatible, y en definitiva todo el texto propuesto por este artículo resulta laudatorio.

El texto del artículo 6º mejora notablemente las propuestas anteriores (el Proyecto Lamorte y el Proyecto Abdala se pronunciaban por la exclusión lisa y llana de los deudores del Estado de este tipo de bases de datos), limitando el registro de morosidades abiertos a la consulta de terceros, con una modulación compatible, a saber:

1º- Prohibición de registro de deudas derivadas del ejercicio de potestades sancionatorias o incumplimiento de pagos de servicios prestados por la Administración.

2º- Excepción a tal prohibición, vale decir posibilidad de registrar la obligación incumplida, cuando exista resolución jurisdiccional firme de condena al pago de la deuda.

Conclusiones

En líneas generales, y sin desmedro de algunas precisiones y observaciones que se han formulado en el cuerpo del Informe, se trata de un Proyecto de Ley que goza de buena técnica y conceptos jurídicos compatibles. De todos los Proyectos en la materia que nos ha tocado opinar, apreciamos que es el mejor logrado. Su texto es adecuado al régimen general de la protección de datos personales estatuido por la Ley Nº 18.331, sus modificativas y reglamentación, perfeccionando -incluso- la normativa vigente.

Fdo. Dr. Marcelo Bauzá

Derechos Ciudadano

Informe solicitado al CERTuy

Informe técnico S/N del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), relativo a las diferentes soluciones técnicas aplicables para que la información personal pueda ser eliminada de los sitios web de un organismo público.

- I- Introducción

A raíz de la solicitud realizada por la Unidad Reguladora y de Control de Protección de Datos Personales, se realizó el análisis de opciones para poder eliminar un contenido de los buscadores de Internet una vez que éste fue indexado y cacheado.

En todos los casos, la persona que publica el contenido tiene que colaborar con su eliminación, no es posible eliminar un contenido particular de internet sin la colaboración (aunque bajo obligación) de la persona que subió el contenido. Un ejemplo claro de eso son los sitios de contenidos multimedia piratas.

El objetivo es entonces determinar si es posible evitar que contenidos que fueron borrados en internet permanezcan indexados y mostrados en los caches de los buscadores de Internet como ser Google, Bing o Yahoo.

- II- Contexto

Los buscadores de Internet (Google, Bing, Yahoo, etc.) periódicamente recorren Internet indexando los contenidos (crawling). De esta forma crean una base de datos para realizar las búsquedas de contenidos en internet. Al mismo tiempo se crea un caché de los contenidos, lo que hace que incluso una vez modificado el sitio real, exista una “copia” con parte del contenido anterior en los sitios de los buscadores.

Esto ocurre para contenidos de texto, no para imágenes o videos ya que en estos últimos solo se indexan las etiquetas (tags) de los mismos. Es entonces importante tener en cuenta que si se quiere aparecer en los buscadores, el contenido tiene que tener texto, ya sea por ser un documento, o porque existen etiquetas de texto que describen a un contenido multimedia.

Agregar las etiquetas manualmente requiere de un esfuerzo extra, ya que hay que hacerlo de forma tal que esas etiquetas sean útiles para describir el contenido del contenido como ser: “resolución”, nombre de la empresa, nombres de los firmantes, título de la resolución, etc.

- III- Análisis

En el escenario antes descrito es importante destacar los siguientes puntos:

- Es necesario ser indexado por los buscadores de Internet en primer lugar para aparecer en los resultados de las búsquedas.

- Si el contenido no es texto, es necesario incorporar etiquetas al contenido de forma manual.
- Cada buscador tiene su propia política de caché, donde en algunos casos es posible advertir que no se quiere cachear el contenido, mientras que en otros casos hay que solicitar que se elimine posteriormente. Incluso en algunos casos no hay forma de prevenir o eliminar el caché.
- Mas allá de los buscadores, un usuario siempre puede copiar el contenido a otro sitio, y en este caso el buscador lo encontrará e indexará en el otro sitio.

Con este escenario, la opción que más aplica para evitar ser cacheado, y que una vez que el contenido se borre no aparezca más en los buscadores, es que los documentos se generen en tiempo real a raíz de peticiones en lugar de que sean documentos generados previamente. De esta forma los buscadores no podrán cachear el contenido porque simplemente no existe en el momento en que consultan. Sin embargo, esto hace necesario que se incluyan etiquetas en los contenidos para que puedan ser indexados y encontrados por los buscadores.

Esta opción sin embargo tiene la desventaja de que no es una solución estándar, y además es necesario agregar las etiquetas manualmente para ser indexados, tarea que no siempre es sencilla y/o viable.

- IV- Conclusión

Dada la complejidad, amplitud y masificación de usuarios de internet, una vez que se sube un contenido, se puede considerar que ya no es posible borrarlo completamente. Para mantener posibilidades de borrar un cierto contenido realmente se tiene que primero haber controlado en cierta forma su copiado y propagación. Para esto existen alternativas que generan el contenido en tiempo real o lo sirven en base a consultas específicas, haciendo que su copiado o indexación sea más compleja, y controlando así su propagación.

El espíritu de los buscadores es que fácilmente se encuentren los contenidos, haciendo la tarea más fácil tanto para quien sube el contenido como para el que lo consume. Al mismo tiempo, los buscadores más populares cuentan con mecanismos para remover los contenidos de los caches. En caso de que ingrese una solicitud de remoción de información del caché de cierto buscador, y que este constate que el sitio original ya no existe, la remoción es prácticamente inmediata. Si la propagación fue controlada en forma adecuada, remover el contenido del sitio original y solicitar la remoción de los cachés de los buscadores puede proveer una posibilidad real de eliminación.

Teniendo en cuenta estos motivos entendemos que la mejor opción es tomar medidas preventivas para controlar la propagación de los documentos, y una vez que se quieren borrar, simplemente borrar el contenido incorrecto de internet y solicitar a los buscadores más populares que lo remuevan de sus cachés. De esta forma se reduce el riesgo de que se encuentre dicho contenido en Internet, quedando como única posibilidad que un usuario lo haya copiado y subido en otro sitio en forma previa. A continuación se presentan los links para

solicitar la baja de los buscadores más populares:

Google

<http://support.google.com/webmasters/bin/answer.py?hl=en&answer=1663660>

Bing

<http://www.bing.com/webmaster/help/block-urls-from-bing-264e560a>

Yahoo

<http://help.yahoo.com//us/yahoo/privacy/access/indexing-13.html>

En todos los casos existe también la posibilidad de utilizar metatags en el código de la página u otros artefactos para evitar ser indexado o cacheado, sin embargo las referencias a estos métodos muestran una tasa de fallo muy grande, por lo que no se recomienda confiar en ellas.



UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES



BICENTENARIO.UY
INSTRUCCIONES
DEL AÑO XIII



agesic

agencia de gobierno electrónico
y sociedad de la información



PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY