Resoluciones, dictámenes e informes 2019

Fecha de creación

20/10/2020

Tipo de publicación

Materiales didácticos

Resumen

Recopilación de resoluciones, dictámenes e informes 2019

Dictámenes

Dictamen N° 1/019, de 15 de enero de 2019. Consulta efectuada por el Instituto Nacional de Inclusión Social (INISA), acerca del procedimiento de intercambio de información entre Entidades Públicas.

Dictamen Nº 2/019, de 12 de marzo de 2019. Consulta remitida por la Dirección Nacional de Aduanas con respecto al alcance del artículo 43 de la Ley N° 19.438, de 14 de octubre de 2016, por el que se faculta a esta Dirección a publicar, entre otra, información de nombres de los importadores y exportadores, además de fechas, número de inscripción en el registro aduanero, valor de aduana, país de origen de destino de las mercaderías.

Dictamen Nº 3/019, de 26 de marzo de 2019. Consulta efectuada por el Área Programática de Adolescencia y Juventud del Ministerio de Salud Pública, acerca de la posibilidad de acceder por la Mesa de Coordinación de Estrategia Territorial y Nacional de Prevención de Embarazo no Intencional en Adolescentes, a los datos necesarios para cumplir con sus objetivos.

Dictamen Nº 4/019, de 2 de abril de 2018. Consulta realizada por la Dra. Virginia Cervieri, por sí y en representación de Estudio Jurídico Cervieri Monsuárez Asociados, acerca de la publicación de informaciones que entiende falsas a través de páginas web paraguayas, a las que es posible acceder desde Uruguay, y que han sido replicadas por medios noticiosos nacionales.

Dictamen Nº 5/019, de 23 de abril de 2019. Consulta realizada por la Unidad Reguladora de Servicios de Comunicaciones (URSEC) acerca de la legalidad que un operador de televisión para abonados del interior del país, coloque cámaras en la vía pública y transmita en vivo durante las 24 horas a través de su canal local.

Dictamen Nº 6/019, de 7 de mayo de 2019. Consulta presentada por el Banco de Previsión Social respecto a la firma de un Acuerdo de Programa con la organización SMILE TRAIN con sede en los Estados Unidos.

Dictamen Nº 7/019, de 14 de mayo de 2019. Consulta acerca del Oficio N° 108/2018-rdjd remitido por la Oficina de Instrucciones Sumariales de la Dirección Nacional Guardia Republicana del Ministerio del Interior.

Dictamen Nº 8/019, de 14 de mayo de 2019. Consulta remitida por el Instituto Nacional de Inclusión Social Adolescente acerca de la compatibilidad entre lo dispuesto en el artículo 24 de la Ley N° 19.367, de 31 de diciembre de 2015 y el proyectado artículo 51 del proyectado Estatuto relativo a la potestad disciplinaria.

Dictamen Nº 9/019, de 27 de agosto de 2019. Consulta realizada por la Facultad de Veterinaria sobre la posibilidad de grabar los exámenes teóricos tomados en modalidad oral.

Dictamen Nº 10/019, de 27 de agosto de 2019. Consulta formulada por el Banco de Previsión Social sobre contestación de oficios judiciales con especial atención a la información referida a montos de prestaciones de actividad y pasividades de afiliados así como otra información de naturaleza sensible.

Dictamen Nº 11/019, de 24 de setiembre de 2019. Consulta remitida por la Secretaría Nacional para la lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAF) acerca de la posibilidad legal de esa Secretaría de publicar las resoluciones que imponen sanciones a los sujetos obligados.

Dictamen Nº 12/019, de 24 de setiembre de 2019. Consulta realizada por el Instituto de Regulación de Cannabis (IRCCA) sobre el tratamiento correcto a conferir a los datos históricos, teniendo en cuenta que la justicia penal podría solicitar datos sobre personas así como la pertinencia de solicitar autorización para la conservación de datos con fines históricos, estadísticos o científicos.

Dictamen Nº 13/019, de 24 de setiembre de 2019. Consulta formulada por la Dirección Nacional de Empleo del Ministerio de Trabajo y Seguridad Social (DINAE) con respecto al Sistema de Intermediación Laboral y la publicación de información de menores de edad.

Dictamen Nº 14/019, de 1 de octubre de 2019. Consulta presentada por el Colegio Nueva Cultura sobre la publicación de informaciones vinculadas a denuncias realizadas por madres de alumnos del colegio, a través de páginas web de medios periodísticos nacionales.

Dictamen Nº 15/019, de 5 de noviembre de 2019. Consulta formulada por el Consejo de Educación Técnico Profesional sobre la posibilidad de contar con una base de datos visible en el sitio web de la institución que contenga identificación de las personas (nombre completo, C.I., título obtenido, nivel que se obtiene con él, plan en que cursó y centro educativo), la situación del trámite del título incluyendo la repartición en que se encuentra y fecha.

Dictamen Nº 16/019, de 5 de noviembre de 2019. Consulta formulada por la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAFT) respecto a una intimación de entrega de copia de resoluciones que aplican sanciones a los sujetos obligados no financieros remitida por el Tribunal de lo Contencioso Administrativo, a requerimiento de la parte actora en un juicio en que la Secretaría es demandada.

Dictamen N° 1/019, de 15 de enero de 2019

Consulta efectuada por el Instituto Nacional de Inclusión Social (INISA), acerca del procedimiento de intercambio de información entre Entidades Públicas.

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

DICTAMEN N°	1	2019
Expediente N°	2018-2-10-000544	

Montevideo, 15 de enero de 2019

VISTO: La consulta realizada por el Instituto Nacional de Inclusión Social (INISA).

RESULTANDO:

1. Que el INISA consulta sobre un procedimiento de intercambio de información entre Entidades Públicas. Expresa que en el marco de la ejecución de convenios entre el Instituto Nacional de la Juventud, el INISA y el Ministerio de Desarrollo Social, se le ha solicitado información de las bases de datos referida a la comisión de infracciones a la ley penal de determinadas personas, a los efectos de que éstas sean atendidas por un programa del MIDES sobre reinserción social.
2. Que a los efectos de complementar la consulta, se solicitó a INISA que agregara toda la documentación existente relacionada con el tema, lo cual fue cumplido en tiempo y forma.
3. Que dentro de la información aportada se encuentra detallada el tipo de datos solicitados: cédulas de identidad, ID del evento, fecha de evento, tipo de delito, rol en la infracción, detalle de la infracción y tipo de medida adoptada. Asimismo, cabe indicar la existencia de un Acuerdo de trabajo con el MIDES para la construcción de un observatorio sobre adolescentes en conflicto con la Ley para la construcción de información técnica en la materia. Y la existencia de un convenio entre MIDES, INJU; INAU e INISA con la finalidad de fortalecer la articulación interinstitucional entre los organismos para abordar la situación de egreso de adolescentes y jóvenes del sistema penal adolescente.

CONSIDERANDO:

1. Que la presente consulta refiere a un intercambio de información privada entre Entidades Públicas. Que el intercambio de información está regulado en los artículos 157 a 160 de la Ley N° 18.719, de 27 de diciembre de 2010, indicando que se deberá promover el intercambio de información o privada autorizada por su titular. Estas mismas normas establecen los principios, el procedimiento y las competencias de AGESIC en este ámbito. Que por su parte, el artículo 3° del Decreto N° 178/013, de 25 de julio de 2013, reglamentario de la citada norma, establece que cuando se trata de información privada debe estarse a lo establecido en la Ley N° 18.331, de 11 de agosto de 2008.
2. Que desde la perspectiva de la protección de datos personales, se está ante una comunicación de datos de acuerdo con el artículo 4° literal b) de la Ley N° 18.331. Que en este marco, el artículo 17 de la misma norma establece que solo se puede comunicar datos personales para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario, y con el previo consentimiento del titular.
3. Que el INISA, conforme con lo establecido en la Ley N° 19.367, de 31 de diciembre de 2005, tiene como objetivo la inserción social y comunitaria de los adolescentes en conflicto con la ley penal. Que por su parte, la Dirección Nacional de Evaluación y Monitoreo del Ministerio de Desarrollo Social tiene como misión ejercer la rectoría en el monitoreo y evaluación de planes, programas, acciones, dispositivos y proyectos sociales en territorio nacional así como su diseño y gestión. Por otro lado, el INJU es el responsable de las políticas sociales nacionales así como de su coordinación, articulación, seguimiento, supervisión y evaluación de los planes, programas y proyectos relacionados con el desarrollo social. Por último, el INAU es el órgano rector en lo que hace relación con las políticas destinadas a promover y proteger a los adolescentes.
4. Que en virtud de lo expresado, existe tanto interés legítimo del emisor como del destinatario para intercambiar información, cuya clara finalidad es brindar políticas sociales tendientes a la reinserción social de los infractores menores de edad. Que en cuanto al consentimiento aplica el artículo 9° de la Ley N° 18.331, por el cual no sería necesario recabarlo por tratarse de funciones propias de los organismos y es información necesaria para el cumplimiento de las funciones legalmente establecidas a cada uno de ellos.
5. Que en cuanto a la consulta relativa a que los datos de la comisión de infracciones penales corresponde considerarlos como datos sensibles, cabe indicar que no se pueden considerar como tales en virtud de que el artículo 4° literal e) de la Ley N 18.331 establece un elenco taxativo que no los incluye. Que si deben ser considerados datos especialmente protegidos por ser una categoría de incluidos dentro del Capítulo IV de la Ley que los regula.
6. Que el INISA cuestiona si está autorizada a comunicar datos personales relativos a la comisión de infracciones a INJU – MIDES tomando en consideración lo dispuesto en el artículo 18 inciso 3° de la Ley N° 18.331. Que a esos efectos, el artículo 96 del Código de la Niñez y la Adolescencia establece la reserva respecto a los medios de comunicación. El artículo 97 del mismo cuerpo normativo regula la reserva del proceso y el artículo 221 refiere a que el INAU será el custodio de la información contenida en el Sistema Nacional de Información sobre Niñez y Adolescencia por lo que se debe garantizar el uso reservado y confidencial de los datos personales. En base a ello, los organismos están habilitados

a comunicar la información pero el tratamiento debe ser confidencial y exclusivamente para las finalidades legalmente impuestas no siendo posible su difusión a terceros.

ATENTO: a lo expuesto y establecido por el artículo 72 de la Constitución de la República, artículos 28, 29 y 31 de la Ley N° 18.331.

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

DICTAMINA:

1. Indicar que resultan de aplicación los artículos 157 a 160 de la Ley N° 18.719, de 27 de diciembre de 2010 así como su decreto reglamentario N° 178/013, así como las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008.
2. Establecer que es posible el intercambio de información en virtud del marco normativo aplicable por el cual se le atribuyen competencias suficientes a las Entidades Públicas intervinientes así como la existencia de convenios entre las partes que establecen los objetos de intercambio.
3. Que los datos relativos a las infracciones penales no son datos sensibles pero si especialmente protegidos por estar dentro del régimen del artículo 18 de la Ley N° 18.331. Que a su respecto debe tenerse en cuenta que la información puede ser intercambiada en forma confidencial, sin revelarse a terceros por ser conveniente según decisión adoptadas por las Entidades participantes.
4. Notifíquese y publíquese

DR. FELIPE ROTONDO

URCDP

Dictamen Nº 2/019, de 12 de marzo de 2019

Consulta remitida por la Dirección Nacional de Aduanas con respecto al alcance del artículo 43 de la Ley N° 19.438, de 14 de octubre de 2016, por el que se faculta a esta Dirección a publicar, entre otra, información de nombres de los importadores y exportadores, además de fechas, número de inscripción en el registro aduanero, valor de aduana, país de origen de destino de las mercaderías.

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

DICTAMEN N°	2	2019
Acta N°	3	2019

Montevideo, 12 de marzo de 2019

VISTO: La consulta recibida de la Dirección Nacional de Aduanas (en adelante DNA) con respecto al alcance del artículo 43 de la Ley N° 19.438, de 14 de octubre de 2016.

RESULTANDO: Que por la Ley mencionada–artículo 43- se faculta a la Dirección Nacional de Aduanas a publicar, entre otra, información de nombres de importadores y exportadores, además de fechas, número de inscripción en el registro aduanero, valor de aduana, país de origen y de destino.

CONSIDERANDO:

1. Que desde la perspectiva de la protección de datos personales, toda revelación de información personal a una persona distinta del titular se configura en una comunicación de datos, regulada expresamente por el artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008. Las hipótesis en las que la comunicación de datos puede realizarse en legal forma se encuentran reguladas en este artículo y en el artículo 9°, por remisión del primero.
2. Que esta Unidad ya se ha pronunciado en dictamen N° 27/013, de 8 de agosto de 2013, N° 1/015 y N° 3/015, ambos del 4 de marzo de 2015. En el punto vinculado a la comunicación de datos de despachantes de aduanas a entidades públicas en el último de esos dictámenes, se expresó que la DNA se encuentra facultada para recolectar y comunicar datos a otros organismos públicos en el cumplimiento de sus funciones, sin requerir para ello del consentimiento de los involucrados, atento a lo establecido en los artículos 9 literal B y 17 literales A y B de la Ley N° 18.331. Con respecto a restantes comunicaciones de datos, ella corresponde según el apartado 1 del dictamen N° 27/013, sólo con el previo consentimiento o luego de la aplicación de mecanismos de disociación, o en su defecto, habilitando la publicación de los datos expresamente mencionados en el literal C del artículo 9° en formato de listado. Esto es reiterado en el dictamen N° 3/015.
3. Que el análisis de pertinencia previo a la comunicación debe realizarse de acuerdo con los principios establecidos en los artículos 6° a 12 de la Ley Nº 18.331, en especial el de finalidad, los cuales deben orientar todo tratamiento de datos, teniendo presente que el derecho a la protección de datos personales es un derecho inherente a la personalidad humana (artículos 1° de esa Ley y 72 de la Constitución).
4. Que en este caso existe una autorización legal para la publicación de la información –siendo de aplicación de lo dispuesto en el artículo 9° literal B por remisión del artículo 17 literal B de la ley citada-, sin perjuicio de lo cual, toda publicación de datos personales –sobre todo si es realizada en internet-, debe basarse en determinados principios y emplear técnicas que mitiguen los impactos eventuales en los derechos de los titulares de esos datos (dictámenes Nº 12/012 de 7 de junio de 2012, 2/014 de 13 de febrero de 2014 y en las Resoluciones Nº 1040/012 de 20 de diciembre de 2012 y 6/016 de 9 de marzo de 2012, entre otras).

ATENTO: A lo expuesto,

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

DICTAMINA:

1. Señalar que la comunicación de datos personales referida por la consultante se encuentra habilitada por ley (artículo 17 literal B y artículo 9° literal B de la Ley N° 18.331, de 11 de agosto de 2008), sin perjuicio de que en forma previa a la publicación, la DIRECCIÓN NACIONAL DE ADUANAS deberá realizar un ejercicio de ponderación de derechos, empleando para ello los criterios recomendados por los dictámenes Nº 12/012 de 7 de junio de 2012, 2/014 de 13 de febrero de 2014 y las Resoluciones Nº 1040/012 de 20 de diciembre de 2012 y 6/016 de 9 de marzo de 2012, entre otras.
2. Comuníquese, publíquese y archívese.

DR. FELIPE ROTONDO

Dictamen Nº 3/019, de 26 de marzo de 2019

Consulta efectuada por el Área Programática de Adolescencia y Juventud del Ministerio de Salud Pública, acerca de la posibilidad de acceder por la Mesa de Coordinación de Estrategia Territorial y Nacional de Prevención de Embarazo no Intencional en Adolescentes, a los datos necesarios para cumplir con sus objetivos.

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

DICTAMEN N°	3 2019
Expediente N°	2018-2-10-000777

Montevideo, 26 marzo de 2019

VISTO: La consulta realizada por el Área Programática de Adolescencia y Juventud del Ministerio de Salud Pública.

RESULTANDO:

1. Que se requiere la opinión de esta Unidad sobre la posibilidad de acceder por parte de la Mesa de coordinación de la estrategia intersectorial y nacional de prevención del embarazo no intencional en adolescentes, a los datos necesarios para cumplir con sus objetivos.
2. Que la Estrategia es una iniciativa impulsada por los Ministerios de Salud Pública, Desarrollo Social, Educación y Cultura, la Oficina de Planeamiento y Presupuesto, la Administración Nacional de Educación Pública, el Instituto del Niño y Adolescente del Uruguay y la Administración de los Servicios de Salud del Estado, con el apoyo del Núcleo Interdisciplinario Adolescencia, Salud y Derechos Sexuales y Reproductivos de la Universidad de la República y del Fondo de Población de las Naciones Unidas.
3. Que la Mesa necesita para cumplir con sus objetivos, acceder a información nominada de los adolescentes de acuerdo con los indicadores de riesgo identificados y plasmados en el documento de la estrategia, a la información identificatoria de las adolescentes que están cursando un embarazo, y a las adolescentes madres, entre otros. Los datos y registros se encuentran dispersos en diferentes sistemas de información de cada una de las sectoriales que integran la estrategia y en otros organismos públicos.

CONSIDERANDO:

1. Que la consulta versa sobre la posibilidad de realizar comunicación de datos personales entre distintas Entidades Públicas por lo que resulta de plena aplicación las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008, sus concordantes y modificativas
2. Que según el artículo 4° literal b) de la citada Ley N° 18.331, se entiende la comunicación de datos como toda revelación de datos realizada a una persona distinta del titular de los datos. Por su parte, el artículo 17 de la misma norma establece que los datos personales sólo podrán ser comunicados *"para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario (…)".*
3. Que es necesario indicar la vigencia de numerosos tratados internacionales en nuestro país relacionados con los Derechos Humanos así como una serie importante de normas relacionadas con la salud sexual y reproductiva en los adolescentes desde distintos enfoques, los cuales fueron oportunamente mencionados en el informe que luce en el presente expediente.
4. Que además cada una de las Entidades involucradas tiene diversas competencias legales que le permiten tener registros de adolescentes en las distintas condiciones mencionadas. En el caso del Ministerio de Salud Pública cuando hace referencia al Área Programática de adolescencia y juventud, el Ministerio de Desarrollo Social cunado hace referencia a formular, ejecutar, supervisar, coordinar, programar, dar seguimiento y evaluar las políticas, estrategias y planes en las áreas de juventud, mujer y familia, adultos mayores, discapacitados y desarrollo social en general; y a diseñar, organizar y operar un sistema de información social con indicadores relevantes sobre los grupos poblacionales en situaciones de vulnerabilidad, que permita la adecuada localización del conjunto de políticas y programas sociales nacionales. Que ASSE posee competencias en cuanto a los datos de salud de las adolescentes embarazadas y que también cuenta con cometidos relacionados con adolescentes en materia educativa el Ministerio de Educación y Cultura así como la Administración Nacional de Educación Pública.
5. Que surge probada la existencia de interés legítimo del emisor y del destinatario para realizar la comunicación de datos. Sin perjuicio de ello, se debe tener en cuenta que el artículo 12 de la Ley N° 18.331, de 11 de agosto de 2008, con la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018, indica que el responsable de la base de datos o tratamiento y el encargado, en su caso, serán responsables de las disposiciones de la Ley. Que, por tanto, se requiere que una de las Entidades involucradas sea la encargada de adoptar todas las medidas necesarias para cumplir con la normativa de protección de datos personales. Que en forma complementara, las distintas Entidades están cumpliendo competencias legalmente establecidas
6. Que resulta necesario indicar que son aplicables los artículos 157 a 160 de la Ley N° 18.719, por las cuales se regula el intercambio de información entre Entidades Públicas. Como en el caso se va a intercambiar información privada se deben tomar en cuenta las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008, modificativas y concordantes y que se

consideran interés que se establezcan los mecanismos o condiciones de éste.

ATENTO: a lo expuesto y establecido por el artículo 72 de la Constitución de la República, artículos 28, 29 y 31 de la Ley N° 18.331.

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

DICTAMINA:

1. Indicar que la comunicación de datos a realizar se considera legítima y cumple con los requisitos establecidos en el artículo 17 de la Ley N° 18.331.
2. Que es necesario que una de las Entidades Públicas sea designada responsable a los efectos de cumplir la normativa de protección de datos personales.
3. Que es necesario tener en cuenta los artículos 157 a 160 de la Ley N° 18.719 en cuanto a la conveniencia de firmar acuerdos de intercambio de información
4. Notifíquese y publíquese.

DR. FELIPE ROTONDO

URCDP

Dictamen Nº 4/019, de 2 de abril de 2018

Consulta realizada por la Dra. Virginia Cervieri, por sí y en representación de Estudio Jurídico Cervieri Monsuárez Asociados, acerca de la publicación de informaciones que entiende falsas a través de páginas web paraguayas, a las que es posible acceder desde Uruguay, y que han sido replicadas por medios noticiosos nacionales.

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

DICTAMEN N°	4	2019
Expediente N°	2018-2-10-000129	

Montevideo, 3 de abril de 2019

VISTO: La consulta realizada por la Dra. Virginia CERVIERI, por sí y en representación de ESTUDIO JURÍDICO CERVIERI MONSUAREZ ASOCIADOS.

RESULTANDO:

1. Que se requiere opinión de esta Unidad sobre la publicación de informaciones que entiende falsas a través de páginas web paraguayas, a las que es posible acceder desde nuestro país, y que han sido replicadas por medios noticiosos en Uruguay. Adjunta medios probatorios de sus dichos.
2. Que se plantean además cuestiones vinculadas al alcance territorial de la normativa nacional y la aplicación del denominado “derecho al olvido”.

CONSIDERANDO:

1. Que el artículo 3° de la Ley N° 18.331, de 11 de agosto de 2008 prevé que *(…) será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado*”. El artículo 12° establece que el responsable de la base de datos es responsable por el cumplimiento de la Ley, sin perjuicio de la responsabilidad que le cabe a los encargados de tratamiento (resolución N° 104/2015, de 23 de diciembre de 2015, Considerando V, entre otros).
2. Que el llamado “derecho al olvido” no posee consagración a nivel nacional, siendo una extensión del derecho de supresión y actualización, en el marco de los principios de finalidad y veracidad consagrados en las normas que regulan la protección de datos personales (artículos 7, 8, 14 y 15 de la Ley Nº 18.331, de 11 de agosto de 2008).
3. Que la Resolución Nº 1040/012 de 20 de diciembre de 2012 propuso soluciones técnicas para evitar la indexación de contenidos e inclusión en el caché de los buscadores y recomendó la aplicación de criterios técnicos para la publicación de contenidos en sitios web. A su vez, el Dictamen Nº 2/014 de 13 de febrero de 2014 señala que es el responsable del contenido del sitio web, quien decida la información a ser publicada, y por cuánto tiempo, al igual que los controles o filtros para evitar la indexación por los motores de búsqueda. Ello fue reiterado en la Resolución Nº 6/016 de 9 de marzo de 2016
4. Que en el dictamen N° 17/2016 se señala que: “*…en la situación planteada por la consultante el titular de los datos incluidos en publicaciones en internet, podrá ejercer el derecho de supresión establecido en el artículo 15 de la Ley Nº 18.331 ante el editor de las páginas web en su calidad de responsable de tratamiento*”.

ATENTO: a lo expuesto e informado,

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

DICTAMINA:

1. En la situación planteada la consultante podrá dirigir el ejercicio de sus derechos ante los responsables o los encargados de tratamiento –incluyendo los motores de búsqueda-, fundado en los artículos 14 y 15 de la Ley N° 18.331, de 11 de agosto de 2008, y en caso de denegación o limitación de sus derechos, plantear la denuncia ante esta Unidad o ante el Poder Judicial en el marco de lo dispuesto en los artículos 34 y 37 y siguientes de la referida Ley.
2. Notifíquese y publíquese.

DR. FELIPE ROTONDO

URCDP

Dictamen Nº 5/019, de 23 de abril de 2019

Consulta realizada por la Unidad Reguladora de Servicios de Comunicaciones (URSEC) acerca de la legalidad que un operador de televisión para abonados del interior del país, coloque cámaras en la vía pública y transmita en vivo durante las 24 horas a través de su canal local.

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

DICTAMEN N°	5	2019
EXPEDIENTE N°	2019-2-10-0000002	

Montevideo, 23 de abril de 2019.

VISTO: La consulta remitida por la Unidad Reguladora de Servicios de Comunicaciones (URSEC).

RESULTANDO: Que específicamente se solicita dictamen en referencia a la consulta que le fuera realizada respecto a la legalidad o no de que un operador de televisión para abonados del interior del país -que identifica-, coloque cámaras en la vía pública y trasmita en vivo durante las 24 horas a través de su canal local.

CONSIDERANDO:

1. Que conforme al art. 4° "D" de la Ley Nº 18.331, de 11 de agosto de 2008 (LPDP), dato personal es toda información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, lo que incluye la imagen.
2. Que el Dictamen N° 10/010, de 16 de abril de 2010 indica que la videovigilancia*"es toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo y esas imágenes constituyen información personal y por tanto será de aplicación la LPDP y sus normas complementarias."*
3. Que la sola reproducción en tiempo real de imágenes captadas por las cámaras supone un tratamiento de datos personales, entendida este 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"* (art. 4° " M" de LPDP).
4. Que la actuación de las personas se encuentra regida por el principio de libertad consagrado en los arts. 7° y 10 de la Constitución, por lo que la limitación al ejercicio de los derechos está dada por leyes establecidas por razones de interés general. La limitación a la colocación de las cámaras, lo está por los requisitos establecidos por la LPDP, en especial los principios que ella explicita.
5. Que la colocación de cámaras de videovigilancia con fines de seguridad pública está atribuida al Ministerio del Interior, y en el caso de contralor del tránsito y policía de espacios públicos, a los Gobiernos Departamentales específicamente como cometidos de la Intendencia, según art. 35 numeral 25 la Ley N° 9.515, en cuanto a la organización y cuidado de la vialidad pública, la que puede ser ejercida mediante la colocación de cámaras (Dictamen N° 15/018, de 04 de setiembre de 2018)
6. Que la colocación de cámaras por particulares en la vía pública tiene los límites establecidos por la LPDP, específicamente la actuación de los responsables de las bases de datos debe ajustarse a los principios de su art. 5° (Legalidad, Veracidad, Finalidad, Previo consentimiento informado, Seguridad de los datos, Reserva y Responsabilidad), y en particular a lo dispuesto en los arts. 6º y 7º.
7. Que de acuerdo con las precitadas disposiciones no resulta viable colocarse cámaras en espacios públicos si captan lugares, personas, matrículas, números de puerta u otro dato similar que identifique o haga identificable a una persona si no se da cumplimiento a la obtención del consentimiento previo, expreso e informado (art 9° y 13 LPDP). Por otra parte, la retrasmisión de las imágenes configura una hipótesis de comunicación de datos en los términos establecidos en el artículo 4 literal B y 17 de la Ley citada.

ATENTO: A lo expuesto,

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

DICTAMINA:

1. Indicar que la colocación de cámaras en la vía pública solo resulta legítima si se da cumplimiento a los principios rectores en materia de protección de datos personales.
2. Señalar que no existe vulneración a la referida protección si las cámaras no permiten la identificación de las personas y se colocan en lugares que capten en forma general la ciudad o son de baja resolución (con aplicación de filtros de privacidad).
3. Señalar que si las cámaras están orientadas a lugares privados y permiten la identificación de las personas, deberá obtenerse su consentimiento previo, expreso e informado e inscribirse la base de datos, además de cumplir el resto de las obligaciones referidas en la Ley Nº 18.331, de 11 de agosto de 2008.

4. Notifíquese, publíquese y oportunamente archívese.

DR. FELIPE ROTONDO

URCDP

Dictamen Nº 6/019, de 7 de mayo de 2019

Consulta presentada por el Banco de Previsión Social respecto a la firma de un Acuerdo de Programa con la organización SMILE TRAIN con sede en los Estados Unidos.

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

DICTAMEN N°	6	2019
EXPEDIENTE N°	2019-2-10-0000079	

Montevideo, 7 de mayo de 2019

VISTO: La consulta presentada por el BANCO DE PREVISIÓN SOCIAL respecto a la firma de un acuerdo de Programa con la organización con sede en los Estados Unidos denominada SMILE TRAIN.

RESULTANDO:

1. Que la consultante solicita a esta Unidad se pronuncie sobre la adecuación a la normativa en materia de protección de datos de las cláusulas del acuerdo que adjunta con SMILE TRAIN -organización sin fines de lucro dedicada a la provisión de fondos, herramientas y educación en materia de labio/paladar hendido-.
2. Que surge de la documentación presentada que el objetivo del acuerdo es concretar esfuerzos de cooperación, permitiendo al BANCO DE PREVISIÓN SOCIAL ofrecer cirugías reconstructivas gratis, entre otros servicios.
3. Que SMILE TRAIN se encuentra ubicada en Nueva York, Estados Unidos de América, y no cuenta con certificación de Privacy Shield.

CONSIDERANDO:

1. Que el presente caso se trata de la aplicación de normativa en materia de transferencias internacionales de datos de salud y de menores de edad a territorio no adecuado, por lo que resulta aplicable la Ley N° 18.331, de 11 de agosto de 2008, en particular sus artículos 17, 18 y 23. Además corresponde la aplicación de los artículos 8° a 12°, este último en la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018.
2. Que el BANCO DE PREVISIÓN SOCIAL tiene cometidos específicos vinculados al tratamiento de las patologías objeto del acuerdo presentado, conforme lo establecido por el Decreto-Ley N° 15.084, de 28 de noviembre de 1980, el decreto N° 227/981, de 27 de mayo de 1981 y demás normas reglamentarias.
3. Que en tanto los padres brinden el consentimiento para la comunicación de la información a SMILE TRAIN, se cumple con lo establecido en el artículo 23 literal A de la Ley N° 18.331, que prevé la transferencia de información con el consentimiento del interesado –en este caso de su representante-. No obstante, deberá revisarse la redacción del modelo de consentimiento –o complementarse en debida forma-, en lo que respecta a la posibilidad de establecerse finalidades adicionales, e informarse que aún en caso de negativa a proporcionar dicho consentimiento, el menor tendrá la posibilidad de obtener la asistencia debida.
4. Que en lo que respecta a la comunicación de información a SMILE TRAIN, deberá limitarse a la estrictamente necesaria para el cumplimiento de las obligaciones asumidas, y asegurarse la supresión de ésta a requerimiento del interesado por una vía sencilla y gratuita. El BANCO DE PREVISIÓN SOCIAL deberá asumir la obligación de recabar esas manifestaciones de voluntad, y que cumpla con lo solicitado por los titulares de los datos o sus representantes.
5. Que en lo que respecta a las restantes obligaciones en el marco del artículo 12° de la Ley N° 18.331, en la redacción dada por el artículo 39 de la Ley N° 19.670, corresponde la realización de una Evaluación de Impacto en la Protección de Datos y el registro de la base de datos de los menores que formen parte del programa.
6. Que atento a lo dispuesto por el artículo 37 literal A de la Ley N° 19.670, SMILE TRAIN se encontrará alcanzada por las disposiciones de la Ley N° 18.331.

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

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. El acuerdo presentado por el BANCO DE PREVISIÓN SOCIAL cumple con las disposiciones en materia de protección de datos para las transferencias internacionales previstas, por encontrarse abarcado en lo dispuesto en el artículo 23 literal A de la Ley N° 18.331, debiendo previamente adaptarse el modelo de consentimiento en la forma indicada en los Considerandos, dando cuenta a esta Unidad.
2. El BANCO DE PREVISIÓN SOCIAL deberá dar cumplimiento a lo dispuesto en el artículo 12° de la Ley N° 18.331, en la redacción dada por el artículo 39 de la Ley N° 19.670, incluyendo las recomendaciones que surgen de los Considerandos del presente Dictamen y lo informado en obrados, dando cuenta a esta Unidad.
3. Notifíquese, publíquese y oportunamente archívese.

DR. FELIPE ROTONDO

URCDP

Dictamen Nº 7/019, de 14 de mayo de 2019

Consulta acerca del Oficio N° 108/2018-rdjd remitido por la Oficina de Instrucciones Sumariales de la Dirección Nacional Guardia Republicana del Ministerio del Interior.

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

DICTAMEN N°	7	2019
EXPEDIENTE N°	2018-2-10-0000659	

Montevideo, 14 de mayo de 2019.

VISTO: El Oficio N° 108/2018-rdjd remitido por la Oficina de Instrucciones Sumariales de la Dirección Nacional Guardia Republicana del Ministerio del Interior.

RESULTANDO:

1. Que en el marco de un Sumario Administrativo dispuesto a un integrante de la Guardia Republicana por una publicación en un grupo de Whatsapp, (creado con la finalidad de coordinar y ver las publicaciones de las órdenes de Servicio) denominado "ART 222", un video en el cual refiere al Señor Presidente de la República y a su familia.
2. Puntualmente, el Instructor sumariante solicita respuesta a las siguientes preguntas*"la siguiente información sobre WhatsApp: a) ¿Es una red social? b) ¿Existe regulación para el uso de una información compartida en los grupos de WhatsApp? En caso positivo ¿cuál es? c) ¿Debe existir consentimiento por parte de quien comparte una información en un grupo de WhatsApp para ser utilizada posteriormente? d) ¿Existe reglamentación que proteja a quien comparte una información, imagen, etc. por WhatsApp? e) ¿Existe reglamentación para proteger la privacidad de lo compartido en un grupo de WhatsApp?*". Solicita además el consultante que *"sin perjuicio de las anteriores preguntas, toda aquella información que puedan aportar al respecto, será de utilidad*" para el Sumario Administrativo.

CONSIDERANDO:

1. Que en lo que refiere a la pregunta a), a nivel normativo no se ha definido qué se entiende por "red social", por lo que se trata de un concepto que debe construirse desde la doctrina. A ese respecto, el Diccionario de la Real Academia Española de la Lengua define en la 23a. acepción del vocablo *"red*" al *"conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información", y, más precisamente, "red social" como "plataforma digital de comunicación global que pone en contacto a gran número de usuarios".*
2. Que en el mismo sentido el Instituto Nacional de Ciberseguridad (INCIBE), ex INTECO, expresa que*"Las redes sociales son espacios virtuales en los que cada usuario cuenta con un perfil público, que refleja datos personales, estado e información de uno mismo. A su vez dispone de herramientas que permiten interactuar y conocer al resto de usuarios, por ejemplo mediante la creación de grupos de interés".* Ahora bien, WhatsApp Messenger es definido como una aplicación de mensajería multiplataforma que permite enviar y recibir mensajes instantáneos a través de un teléfono móvil y posibilita el intercambio de textos, audios, videos y fotografías; cuenta en la actualidad con cifrado de extremo a extremo de la comunicación que evita que terceros accedan al contenido de esta. Se requiere la creación de un perfil y permite interactuar con otros usuarios o grupos. Por tanto, cumple con las características de una red social.
3. Que respecto de la pregunta b), es de aplicación a la información (mensajes, fotografías, videos) compartida a través de WhatsApp, el marco jurídico dado por la Constitución de la República, en lo que refiere a libertad de expresión, de asociación, inviolabilidad de la correspondencia, protección de datos personales, así como la normativa específica relativa a la difamación e injurias cuando correspondiere. Alcanza también a la información compartida por WhatsApp la normativa de derechos de propiedad intelectual, derechos de autor y marcas registradas, en lo que sea aplicable. El funcionamiento a nivel interno de un grupo de WhatsApp -más allá de la normativa antes reseñada-, es de resorte exclusivo de sus creadores y participantes por lo que la forma de ingreso, el tipo de información, lenguaje, será determinado de forma autorregulada por su administrador/creador y por los términos y condiciones de uso propios de WhatsApp.
4. Que en cuanto a la pregunta c), cabe indicar que quien comparte información en WhatsApp queda comprendido en lo establecido en los artículo 4° literal B) y artículo 17 de la Ley N° 18.331 de 11 de agosto de 2008, y por tanto, si una persona envía información propia a un grupo de WhatsApp, está prestando su consentimiento para su utilización en el marco de dicho grupo (artículo 9° de la citada Ley), y con una finalidad determinada. En virtud de ello, utilizarla más allá de ese ámbito implica comunicar datos sin previo consentimiento e infringiendo el principio de finalidad.
5. Que en cuanto a la pregunta d), resulta de aplicación a la información compartida por WhatsApp, además de la normativa antes reseñada, la Ley N° 9.739 de 12 de diciembre de 1937 por la cual se protegen los Derechos de Autor y la Ley N° 17.616, de 10 de enero de 2003, de Protección de la Propiedad Intelectual, en lo que corresponda.
6. Que respecto a la pregunta e), se indica que es de aplicación la Ley N° 18.331, de 11 de agosto de 2008, en lo relativo al consentimiento y comunicación de datos, para proteger la privacidad de lo compartido en un grupo de WhatsApp.

ATENTO: A lo expuesto y lo dispuesto por los artículos citados,

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

DICTAMINA:

1. Expedirse en el sentido indicado en los Considerandos I a VI del presente dictamen.
2. Notifíquese, publíquese y oportunamente archívese.

DR. FELIPE ROTONDO

URCDP

Dictamen Nº 8/019, de 14 de mayo de 2019

Consulta remitida por el Instituto Nacional de Inclusión Social Adolescente acerca de la compatibilidad entre lo dispuesto en el artículo 24 de la Ley N° 19.367, de 31 de diciembre de 2015 y el proyectado artículo 51 del proyectado Estatuto relativo a la potestad disciplinaria.

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

DICTAMEN N°	8	2019
Expediente N°	2018-2-10-000347	

Montevideo, 14 de mayo de 2019

VISTO: La consulta remitida por el Instituto Nacional del de Inclusión Social Adolescente.

RESULTANDO:

1. Que en el marco de lo dispuesto en el artículo 24 de la Ley N° 19.367, de 31 de diciembre de 2015, surge una diferencia de visión respecto de la redacción del artículo 51 del proyectado Estatuto relativo a la potestad disciplinaria; especialmente respecto al inciso final, cuyo texto reza: "*Exceptúase la participación y acceso a las declaraciones de los adolescentes y jóvenes atendidos en el Instituto, así como cualquier otro dato relativo a ellos para el sumariado, de conformidad con la Ley 18.381 y Ley 19.178*".
2. Que se realizó consulta a la Asesoría de la Oficina Nacional de Servicio Civil, la que estimó que era necesario que el funcionario y su abogado patrocinante tuvieran acceso a todas las declaraciones para una mejor defensa, en pos de la sustanciación del debido proceso. En forma similar opinó el Sindicato, que además propuso una redacción alternativa.

CONSIDERANDO:

1. Que el presente caso involucra el tratamiento de datos personales de diversas personas en un sumario administrativo, incluidas menores de edad y jóvenes, por lo que resulta de plena aplicación lo dispuesto en la Ley N° 18.331, de 11 de agosto de 2008.
2. Que a los efectos de poder determinar si procede el acceso a la información por parte del sumariante y su patrocinante, es necesario tomar en cuenta dos elementos sustanciales que se encuentran en juego: el debido proceso y el interés superior del menor.
3. Que con respecto al primero, es una garantía esencial en un Estado de Derecho, consagrada en los arts. 12 de la Constitución y 8° del Pacto de San José de Costa Rica.

Si no se accede a la información de que se trata, se estaría ante la posibilidad de vulnerar el debido proceso, siendo aplicable el artículo 7° de la Carta que establece que solamente los límites a los derechos deben provenir de una ley y por razones de interés general. Por otro lado, se aprecia el interés superior del menor, reconocido en la mayoría de los instrumentos internacionales de los cuáles Uruguay forma parte y normas de menos valor y fuerza.

4. Que, por tanto, resulta pertinente la ponderación de los referidos elementos y como resultado, corresponde pronunciarse por la prevalencia de debido proceso por su especial vínculo con la libertad de la persona. Sin perjuicio de ello, como alternativa, cabe establecer un procedimiento para acceder a la información, basado en ley que protege los bienes jurídicos presentes; así se pueden determinar algunas características, como las de que la información sea tratada en forma individual y reservada, sin presencia de representantes de la persona denunciada ni de los denunciantes y sin identificar en el expediente los datos de los declarantes. La información recaba puede ser resguardada fuera del expediente y permanecer a cargo de la entidad durante un plazo a establecer, para el caso que así lo solicite la sede judicial, con lo cual cumpliría con el principio de reserva regulado en el artículo 11 de la Ley N° 18.331, de 11 de agosto de 2008.
5. Que otro principio a considerar es el de finalidad por el cual los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su atención.
6. Que otro elemento de importancia es que en el tratamiento de datos personales se utilicen criterios de disociación. A esos efectos, la Unidad mediante la Resolución 68/017, de 26 de abril de 2017, aprobó el documento *"Criterios de disociación de datos personales*" por el cual se establecen diversos mecanismos de disociación de datos personales.
7. Que se considera adecuado que en todo lo que hace relación con la clasificación de la información, se remita consulta a la Unidad de Acceso a la Información Pública, como órgano rector en la materia.

ATENTO: a lo expuesto e informado.

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

DICTAMINA:

1) En la consulta planteada se está ante un caso de ponderación de derechos y que se estime pertinente garantizar el debido proceso y si interés superior del menor salvo que se establezca por vía legislativa un procedimiento para la entrega de la información, indicando además la forma de tratar los datos personales.

2) La información deberá ser tratada de conformidad con los principios de la protección de datos personales, en especial énfasis en la reserva y la finalidad, debiendo tenerse presente los Criterios de Disociación de Personales como herramienta para disociar la información.

3) Notifíquese y publíquese.

DR. FELIPE ROTONDO

URCDP

Dictamen Nº 9/019, de 27 de agosto de 2019

Consulta realizada por la Facultad de Veterinaria sobre la posibilidad de grabar los exámenes teóricos tomados en modalidad oral.

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

Dictamen Nº	9	2019
Expediente Nº	2019-2-10-0000070	

Montevideo, 13 de agosto de 2019.

VISTO: La consulta formulada por la FACULTAD DE VETERINARIA sobre la posibilidad de grabar los exámenes teóricos tomados en modalidad oral

RESULTANDO:

1. Que el planteo de la consultante se fundamenta en la solicitud realizada por estudiantes y docentes de la Facultad citada, y que fuera elevado a la Comisión de Enseñanza.
2. Que la consultante adjunta informe de la Dirección General Jurídica de la Universidad de la República, en el que se esgrime la posibilidad de aplicar las definiciones existentes en el Dictamen N° 10/010 de 16 de abril de 2010 del Consejo Ejecutivo de la Unidad, respecto al tema de videovigilancia.

CONSIDERANDO:

1. Que corresponde considerar la aplicación del artículo 9° de la Ley N° 18.331, de 11 de agosto de 2008, que prevé el consentimiento previo, expreso e informado de los titulares de los datos y otras bases legítimas del tratamiento –calificadas como excepciones al principio del previo consentimiento informado-. No es necesario en consecuencia el consentimiento, cuando el tratamiento se encuentra alcanzado por las excepciones expresamente previstas en la norma.
2. Que son aplicables además, la Ley N° 12.549 de 29 de octubre de 1958 (Ley Orgánica de la Universidad de la República), el Reglamento de 27 de diciembre de 1967 aprobado por el Consejo Directivo Central para la Facultad de Veterinaria y la Ordenanza de Estudios de Grado y Otros Programas de Formación Terciaria (Res. Nº 3 de C.D.C. de 2/VIII/2011 – Dist. Nº 451/11, Res. Nº 4 del C.D.C. de 30/VIII/2011– Dist. Nº 575/11 y 576/11, publicada en el Diario Oficial el 19 de setiembre de 2011).
3. Que del análisis de las normas resulta que resulta necesaria su armonización a efectos de homogeneizar el tratamiento de los datos personales, aunque no resulta necesario el consentimiento previo, expreso e informado de los estudiantes y docentes para la grabación de los exámenes orales si así lo disponen los reglamentos que se dicten a nivel universitario y se establecen medios para garantizar un adecuado tratamiento de los datos personales.

ATENTO: A lo expuesto y lo dispuesto por los artículos mencionados,

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

DICTAMINA:

1. La grabación de los exámenes orales y su almacenamiento no vulnera las normas en materia de protección de datos personales si así lo establecen los reglamentos a nivel universitario.
2. El tratamiento de los datos referido en el numeral anterior deberá realizarse al amparo de lo establecido en la Ley N° 18.331, de 11 de agosto de 2008, dando cumplimiento a los principios en ella establecidos.

MAG. FEDERICO MONTEVERDE

URCDP

Dictamen Nº 10/019, de 27 de agosto de 2019

Consulta formulada por el Banco de Previsión Social sobre contestación de oficios judiciales con especial atención a la información referida a montos de prestaciones de actividad y pasividades de afiliados así como otra información de naturaleza sensible.

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

DICTAMEN N°	10	2019
EXPEDIENTE N°	2018-2-10-0000653	

Montevideo, 27 de agosto de 2019.

VISTO: La consulta formulada por el BANCO DE PREVISIÓN SOCIAL sobre contestación de oficios judiciales.

RESULTANDO: Que el consultante solicita pronunciamiento de esta Unidad con respecto a la aplicación de las normas en materia de protección de datos personales a las contestaciones de oficios recibidos del poder judicial, con especial atención a la información de montos de prestaciones de actividad y pasividad de afiliados y otra información de naturaleza sensible.

CONSIDERANDO:

1. Que en la situación de prestaciones de actividad y pasividad es de aplicación lo dispuesto por el artículo 47 del Código Tributario del Uruguay, no siendo por ende los datos abarcados por dicho artículo confidenciales sino secretos.
2. Que con respecto a los datos sensibles, resultan de aplicación en la especie los artículos 17 y 18 de la ley N° 18.331, de 11 de agosto de 2008, en los que se prevé distintas hipótesis para la comunicación de los datos, que no se limitan al consentimiento previo, expreso y en su caso escrito del titular del dato. En consecuencia, si existe un interés por parte del Juzgado correspondiente, reflejado en un oficio, con determinación de la información solicitada, su fin y aplicación a un proceso determinado, corresponderá su entrega.

ATENTO: A lo expuesto y lo dispuesto por los artículos mencionados,

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

DICTAMINA:

1. La información asociada al pago de los tributos recaudados por la consultante se encuentra abarcada por las disposiciones en materia de secreto tributario y por ende sólo podrá ser entregada –aún al Poder Judicial- en los casos expresamente previstos en la norma.
2. Toda otra información fuera de la mencionada en el literal anterior, aún de naturaleza sensible, podrá ser entregada a requerimiento del Poder Judicial, aún sin contar con consentimiento expreso y por escrito del interesado, siempre que se acrediten las condiciones establecidas en el artículo 17 literal B y en el artículo 9 literal B de la Ley N° 18.331, de 11 de agosto de 2008.

MAG. FEDERICO MONTEVERDE

URCDP

Dictamen Nº 11/019, de 24 de setiembre de 2019

Consulta remitida por la Secretaría Nacional para la lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAF) acerca de la posibilidad legal de esa Secretaría de publicar las resoluciones que imponen sanciones a los sujetos obligados.

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

DICTAMEN N°	11	2019
Expediente N°	2019-2-10-0000345	

Montevideo, 24 de setiembre de 2019

VISTO: La consulta remitida por la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (en adelante SENACLAFT).

RESULTANDO:

1. Que en el marco de lo dispuesto en el artículo 4° y 13 de la Ley N° 19.574, de 20 de diciembre de 2017, se establece dentro de los cometidos de la SENACLAFT el control del cumplimiento de las normas de prevención de lavado de activos y financiamiento del terrorismo así como ejecutar las sanciones pecuniarias impuestas.
2. El procedimiento administrativo tendiente a la aplicación de las referidas sanciones se tramita por el Decreto N° 500/991, culminando –de corresponder- con la aplicación de una sanción de apercibimiento, observación, multa o suspensión o en su caso el archivo, previo conocimiento del interesado.

CONSIDERANDO:

1. Que la consulta involucra el tratamiento de datos personales de diversas personas físicas o jurídicas, por lo que resulta de aplicación lo dispuesto en la Ley N° 18.331, de 11 de agosto de 2008.
2. Que a los efectos de determinar si procede la publicación de las resoluciones es preciso tomar en cuenta lo establecido en los artículos 4° literal B, 17 y 18 de la Ley N° 18.331 (comunicación de datos, previo consentimiento informado, datos especialmente protegidos). En particular, corresponde analizar la ponderación de los derechos en conflicto (transparencia de las sanciones y facultad conferida a las entidades públicas en general en el artículo 18 in fine de la Ley N° 18.331 por un lado, y derecho de la persona a que dicha información no quede a perpetuidad por otro).
3. Que además, todo tratamiento de datos, incluyendo su comunicación, deberá ajustarse a los principios establecidos en la Ley N° 18.331, sin perjuicio de la clasificación o calificación que se realice por parte de SENACLAFT de la información contenida en el expediente en el marco de lo dispuesto por la Ley N° 18.381, de 17 de octubre de 2008.
4. Que en lo que refiere a la publicación de sanciones en internet, corresponde considerar los criterios indicados en la Resolución N° 1040/2012 de esta Unidad, de fecha 20 de diciembre de 2012.

ATENTO: a lo expuesto.

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

DICTAMINA:

1. Resulta aplicable a la situación detallada en la consulta, la excepción al principio del previo consentimiento informado indicada en el art. 18 in fine de la Ley N° 18.331, de 11 de agosto de 2008 (infracciones penales, civiles o administrativas). La responsabilidad por la valoración en la publicación en caso de no existir norma específica corresponde a la entidad que la pública (en el caso SENACLAFT).
2. Los datos personales deberán ser tratados de conformidad con los restantes principios de la protección de datos personales, debiendo tener presente en particular lo indicado en la Resolución N° 1040/2012 de esta Unidad, de fecha 20 de diciembre de 2012.
3. Notifíquese y publíquese.

MAG. FEDERICO MONTEVERDE

URCDP

Dictamen Nº 12/019, de 24 de setiembre de 2019

Consulta realizada por el Instituto de Regulación de Cannabis (IRCCA) sobre el tratamiento correcto a conferir a los datos históricos, teniendo en cuenta que la justicia penal podría solicitar datos sobre personas así como la pertinencia de solicitar autorización para la conservación de datos con fines históricos, estadísticos o científicos.

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

DICTAMEN N°	12	2019
Expediente N°	2019-2-10-0000240	

Montevideo, 24 de setiembre de 2019

VISTO: La consulta realizada por el INSTITUTO DE REGULACIÓN Y CONTROL DE CANNABIS (en adelante IRCCA).

RESULTANDO:

1. Que el IRCCA indica que es responsable de una base de datos que se encuentra registrada ante la Unidad Reguladora y de Control de Datos Personales, y que los datos concretos que se asientan en dicha base (adquirientes de cannabis locales de expendio, cultivadores domésticos y miembros de los Clubes Cannábicos de Membresía) son considerados datos sensibles de acuerdo con lo dispuesto en el artículo 3° del Decreto Ley N° 14.294, en la redacción dada por el artículo 5° de la Ley N° 19.172, de 20 de diciembre de 2013.
2. Que, en ese marco, requiere la opinión de la Unidad sobre dos aspectos: a) el tratamiento correcto a conferir a los datos históricos, teniendo presente que la Justicia Penal puede llegar a solicitar datos sobre personas; b) si el IRCCA debe solicitar autorización para la conservación de datos con fines históricos, estadísticos o científicos.

CONSIDERANDO:

1. Que conforme a la Ley N° 19.172, de 20 de diciembre de 2013, se pretende promover y mejorar la salud pública de la población mediante una política orientada a minimizar los riesgos y a reducir los daños del uso del cannabis. La norma crea el IRCCA como persona pública no estatal, encargada de todos los temas vinculados al uso de cannabis.
2. Que, conforme con el artículo 8 de la ley citada, se crea un registro que *"..llevará sendos registros para las excepciones previstas en los literales A), B), C), D), E), F) y G) del artículo 3° del Decreto-Ley N° 14.294, de 31 de octubre de 1974, en la redacción dada por el artículo 5° de la presente ley (…)".* Esta norma fue posteriormente reglamentada por los decretos Nº 128/016 de 02 de mayo de 2016, Nº 46/015 de 04 de febrero de 2015, Nº 372/014 de 16 de diciembre de 2014 y Nº 120/014 de 06 de mayo de 2014 (este último regula en sus artículos 52 a 77 el *"Registro del Cannabis").*
3. Que resulta de aplicación al caso concreto la Ley N° 18.331, ya que se trata de la posibilidad de conservar datos personales declarados sensibles de acuerdo con el artículo 8° de la Ley N° 19.172, con la potencialidad de ser comunicados a la Justicia Penal.
4. Que, en cuanto a la conservación, se debe considerar el artículo 8° de la Lay N° 18.331 que establece con carácter general en su inciso primero que "*Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados."***.** No obstante, corresponde señalar que el Decreto N° 120/014, establece en las distintas secciones del Registro criterios para la conservación de los datos personales (artículos 52 en adelante).
5. Que en los casos en que existan razones legales suficientes, se podrán conservar los datos previo bloqueo (definido por el artículo 4° del decreto N° 414/009 como *"procedimiento mediante el cual se reservan datos con el fin de impedir su tratamiento, excepto para ser puestos a disposición de los Poderes del Estado, o instituciones que estén legalmente habilitadas, a los efectos de atender las posibles responsabilidades surgidas del tratamiento"*).
6. Que, transcurrido el plazo referido en el considerando anterior, corresponde la eliminación de toda la información, salvo que se acrediten razones históricas, estadísticas o científicas basadas en la legislación específica que permitan su conservación para lo cual deberá seguirse el procedimiento previsto en el artículo 37 del Decreto N° 414/009.
7. Que en lo que refiere a la entrega de información solicitada por la Justicia Penal, es de aplicación el Dictamen N° 16/2018, de 11 de setiembre de 2018 de esta Unidad, conforme el cual se deberá proceder a la entrega de la información cuando ésta efectivamente exista, indicándose en caso contrario que no existe la información solicitada por la causal que corresponda al caso concreto (vencimiento del plazo, sanción, etc.).

ATENTO: a lo expuesto e informado,

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

DICTAMINA:

1. En relación con la primera consulta, corresponde la aplicación del artículo 8° de la Ley N° 18.331, por lo que los datos se pueden conservar en tanto existan las razones por las cuales se recolectaron. La normativa específica que regula los distintos sectores que conforman el Registro de Cannabis prevé plazos especiales de conservación que deberán ser

respetados.

2. Para la conservación de los datos más allá de la finalidad para la que fueron recolectados debe existir un fundamento legal y realizarse un bloqueo previo. Vencidos todos los plazos, se debe proceder a su eliminación, pudiendo conservarlos solamente por razones históricas, científicas o estadísticas, siguiendo el procedimiento establecido a esos efectos por el artículo 37 del Decreto N° 414/009.
3. Notifíquese y publíquese.

MAG. FEDERICO MONTEVERDE

URCDP

Dictamen Nº 13/019, de 24 de setiembre de 2019

Consulta formulada por la Dirección Nacional de Empleo del Ministerio de Trabajo y Seguridad Social (DINAE) con respecto al Sistema de Intermediación Laboral y la publicación de información de menores de edad.

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

Dictamen N°	13	2019
Expediente N°	2019-2-10-0000252	

Montevideo, 24 de setiembre de 2019

VISTO: La consulta realizada por la Dirección Nacional de Empleo (en adelante DINAE) del Ministerio de Trabajo y Seguridad Social con respecto al Sistema de Intermediación Laboral y la publicación de información de menores de edad.

RESULTANDO: Que la consulta versa sobre la aplicabilidad de la Ley N° 18.331, de 11 de agosto de 2008, a la información publicada por menores de edad en el perfil del sistema de intermediación laboral web desarrollado por la DINAE y el Instituto Nacional de Empleo y Formación Profesional (INEFOP), disponible a través de la Plataforma Vía Trabajo.

CONSIDERANDO:

1. Que en el presente caso resultan aplicables las disposiciones de la Ley N° 18.331, y los artículos 213 y siguientes del Código Civil (en especial el artículo 267 referente al peculio industrial, entre otros), el Código de la Niñez y la Adolescencia (en particular el Capítulo XII, artículos 161 a 180) y la Ley N° 19.133, de 20 de setiembre de 2013, sobre fomento del empleo juvenil.
2. Que el derecho a la protección de datos personales es un derecho fundamental reconocido en el artículo 1° de la Ley N° 18.331, y se sustenta en varios principios, entre los que se encuentra el del previo consentimiento informado (artículo 9°). Este principio sienta varias bases legítimas de tratamiento de los datos estableciendo al previo consentimiento como la principal, pero regulando otras en la forma de excepciones.
3. Que no existen normas específicas que regulen el consentimiento de menores de edad e incapaces en lo que respecta a la protección de sus datos personales, por lo que deberá acudirse a las normas en materia de representación previstas en el derecho civil.
4. Que, en el caso específico del desarrollo de tareas laborales, el consentimiento de los adolescentes habilitados por las normas para trabajar no es suficiente, debiendo complementarse con el de sus progenitores –conforme lo indicado en los artículos 167 del Código de la Niñez y de la Adolescencia y 7° de la Ley N° 19.133-.
5. Que, sin perjuicio de tratarse de derechos diferentes, en el caso concreto de obrados el consentimiento referido en el considerando anterior resulta comprensivo del requerido para la publicación de la información en la plataforma referida.

ATENTO: a lo expuesto e informado,

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

DICTAMINA:

1. El consentimiento de los representantes de los menores de edad habilitados por las normas para trabajar, para la publicación de información vinculada a su experiencia y preparación laboral exclusivamente en el Portal Vía Trabajo, se encuentra incluido en el consentimiento otorgado para el cumplimiento de las tareas laborales, reflejado en el carné de habilitación laboral.
2. El Ministerio de Trabajo y Seguridad Social deberá arbitrar todas las medidas necesarias para el cumplimiento de los principios de la Ley N° 18.331 en la publicación de datos de los menores de edad en el Portal Vía Trabajo, con la asistencia y colaboración de las instituciones vinculadas a la defensa de dichos menores.
3. Notifíquese y publíquese.

MAG. FEDERICO MONTEVERDE

URCDP

Dictamen Nº 14/019, de 1 de octubre de 2019

Consulta presentada por el Colegio Nueva Cultura sobre la publicación de informaciones vinculadas a denuncias realizadas por madres de alumnos del colegio, a través de páginas web de medios periodísticos nacionales.

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

DICTAMEN N°	14	2019
Expediente N°	2019-2-10-000338	

Montevideo, 1 de octubre de 2019

VISTO: La consulta realizada por el COLEGIO NUEVA CULTURA.

RESULTANDO: Que se requiere opinión de esta Unidad sobre la publicación de informaciones vinculadas a denuncias realizadas por madres de alumnos del colegio, a través de páginas web de medios periodísticos nacionales.

CONSIDERANDO:

1. Que el artículo 3° de la Ley N° 18.331, de 11 de agosto de 2008 prevé que "*(…) será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado*". El artículo 12° establece que el responsable de la base de datos es responsable por el cumplimiento de la Ley, sin perjuicio de la responsabilidad que le cabe a los encargados de tratamiento (resolución N° 104/2015, de 23 de diciembre de 2015, Considerando V, entre otros).
2. Que el llamado "derecho al olvido" no posee consagración a nivel nacional, siendo una extensión del derecho de supresión y actualización, en el marco de los principios de finalidad y veracidad consagrados en las normas que regulan la protección de datos personales (artículos 7, 8, 14 y 15 de la Ley Nº 18.331, de 11 de agosto de 2008).
3. Que la Resolución Nº 1040/012 de 20 de diciembre de 2012 propuso soluciones técnicas para evitar la indexación de contenidos e inclusión en el caché de los buscadores y recomendó la aplicación de criterios técnicos para la publicación de contenidos en sitios web. A su vez, el Dictamen Nº 2/014 de 13 de febrero de 2014 señala que es el responsable del contenido del sitio web, quien decida la información a ser publicada, y por cuánto tiempo, al igual que los controles o filtros para evitar la indexación por los motores de búsqueda. Ello fue reiterado en la Resolución Nº 6/016 de 9 de marzo de 2016.
4. Que en el dictamen N° 17/2016 se señala que: "*…en la situación planteada por la consultante el titular de los datos incluidos en publicaciones en internet, podrá ejercer el derecho de supresión establecido en el artículo 15 de la Ley Nº 18.331 ante el editor de las páginas web en su calidad de responsable de tratamiento*".
5. Que en el caso de información publicada por medios de prensa, es necesario realizar una ponderación de derechos, por no ser los derechos reconocidos por la Constitución absoluto conforme jurisprudencia de la Suprema Corte de Justicia. Ese ejercicio de ponderación corresponde en primer lugar a los responsables y encargados en su caso, sin perjuicio de la actuación del Poder Judicial cuando la naturaleza de los derechos en conflicto lo amerite.

ATENTO: a lo expuesto e informado,

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

DICTAMINA:

1. En la situación planteada el consultante podrá dirigir el ejercicio de sus derechos ante los responsables o los encargados de tratamiento –incluyendo los motores de búsqueda-, fundado en los artículos 14 y 15 de la Ley N° 18.331, de 11 de agosto de 2008, que podrán aplicar los mecanismos mencionados en el Considerando III.
2. En caso de denegación o limitación de sus derechos, el consultante podrá plantear la denuncia ante esta Unidad o ante el Poder Judicial en el marco de lo dispuesto en los artículos 34 y 37 y siguientes de la referida Ley.
3. Notifíquese y publíquese

MAG. FEDERICO MONTEVERDE

URCDP

Dictamen Nº 15/019, de 5 de noviembre de 2019

Consulta formulada por el Consejo de Educación Técnico Profesional sobre la posibilidad de contar con una base de datos visible en el sitio web de la institución que contenga identificación de las personas (nombre completo, C.I., título obtenido, nivel que se obtiene con él, plan en que cursó y centro educativo), la situación del trámite del título incluyendo la repartición en que se encuentra y fecha.

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

DICTAMEN N°	15	2019
Expediente N°	2019-2-10-0000340	

Montevideo, 5 de noviembre de 2019

VISTO: La consulta realizada por el Consejo de Educación Técnico Profesional.

RESULTANDO:

1. Que la Unidad de Prosecretaria del Consejo de Educación Técnico Profesional consulta sobre la posibilidad de contar con una base de datos visible en el sitio web de la institución que contenga identificación de la persona con nombre completo, cédula de identidad, título obtenido, nivel que se obtiene el mismo, plan en que cursó y centro educativo. Asimismo, el trámite del título con la repartición en que se encuentra y fecha.
2. Que además agrega que sería un apartado en el sitio web al que se accedería ingresando el nombre de la persona o su cédula de identidad, y se desplegaría una ventana con los datos antes referidos. En ese marco, solicita conocer si para instrumentar una base de datos de este tenor, se requiere el previo consentimiento a efectos de proceder a publicar esos datos personales.

CONSIDERANDO:

1. Que el presente caso refiere a la legalidad de realizar una comunicación de datos, definida en el artículo 4° literal b) de la Ley N° 18.331, de 11 de agosto de 2008.
2. Que para realizar dicha comunicación el artículo 17 de la misma norma indica que los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, salvo excepciones que en este caso no resultan aplicables.
3. Que otro aspecto de análisis es el impacto de la publicación en Internet de este tipo de datos. Que se debe tener en cuenta el principio de veracidad (artículo 7° de la Ley N° 18.331), indicando que los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la que se obtuvieron. Que, desde esta perspectiva, al no ser aplicable ninguna de las excepciones establecidas, ni normas que mandaten su publicación, no corresponde la publicación sin el consentimiento de los titulares.
4. Que conforme con las modificaciones introducidas por la Ley N° 19.670, específicamente el nuevo artículo 39, los responsables y encargados de bases de datos deben adoptar las medidas técnicas y organizativas que correspondan para asegurar su protección (privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, etc.).

ATENTO: a lo expuesto y establecido por el artículo 72 de la Constitución de la República, artículos 28, 29 y 31 de la Ley N° 18.331.

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

DICTAMINA:

1. Que a los efectos de la publicación de la información referida en estos procedimientos en Internet, es necesario recabar el previo consentimiento informado de los titulares de los datos por no resultar aplicable ninguna de las excepciones previstas en la Ley N° 18.331, de 11 de agosto de 2008.
2. Que el tratamiento de los datos deberá ajustarse a los principios de la normativa de protección de datos personales en la forma indicada en el presente Dictamen,
3. NOTIFÍQUESE Y PUBLÍQUESE

MAG. FEDERICO MONTEVERDE

URCDP

Dictamen Nº 16/019, de 5 de noviembre de 2019

Consulta formulada por la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAFT) respecto a una intimación de entrega de copia de resoluciones que aplican sanciones a los sujetos obligados no financieros remitida por el Tribunal de lo Contencioso Administrativo, a requerimiento de la parte actora en un juicio en que la Secretaría es demandada.

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

DICTAMEN N°	16	2019
Expediente N°	2019-2-10-0000448	

Montevideo, 5 de noviembre de 2019

VISTO: La consulta realizada por la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (en adelante SENACLAFT);

RESULTANDO:

1. Que la SENACLAFT consulta respecto a una intimación de entrega de copia de resoluciones que aplican sanciones a los sujetos obligados no financieros remitida por el Tribunal de lo Contencioso Administrativo, a requerimiento de la parte actora en un juicio en que la Secretaría es demandada.
2. Que las referidas resoluciones contienen datos personales (nombres y documentos) tanto de los sujetos obligados como de sus clientes, por lo que la Secretaría considera oportuno recabar la opinión de esta Unidad a efectos de conocer la aplicabilidad de las normas en materia de protección de datos.

CONSIDERANDO:

1. Que la situación planteada refiere a una comunicación de datos (artículo 4° literal b) de la Ley N° 18.331, de 11 de agosto de 2008). El artículo 17 de la citada norma establece que sólo podrán ser comunicados los datos personales 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 –salvo excepciones expresamente previstas en dicho artículo y en el artículo 9° de la Ley-.
2. Que corresponde considerar además el artículo 18 de la Ley citada en cuanto establece:*"Los datos relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas, sin perjuicio de las autorizaciones que la ley otorga u otorgare. Nada de lo establecido en esta ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren inconveniente"*.
3. Que el artículo 4 de la Ley N° 19.574, de 20 de diciembre de 2017, establece que la SENACLAFT es un órgano desconcentrado dependiente directamente de la Presidencia de la República, con autonomía técnica, y que posee entre sus cometidos: *"E) El control del cumplimiento de las normas de prevención de lavado de activos y financiamiento del terrorismo por parte de los sujetos obligados por el artículo 13 de la presente ley. (…) H) Ejecutar las sanciones pecuniarias que imponga mediante resolución…".* Por tanto, en este caso la solicitud de información es realizada a la Entidad Pública competente para brindarla.
4. Que el Tribunal de lo Contencioso Administrativo es un órgano jurisdiccional que tiene como cometido resolver las demandas de nulidad de los actos generales que dicte la Administración (artículo 25 de la Ley N° 15.524) y ha sido opinión firme de esta Unidad, que cuando la información sea solicitada en el marco de una función jurisdiccional, ésta debe ser entregada. Corresponde considerar especialmente la opinión reflejada en Dictamen N° 10/019 de 27 de agosto de 2019 del Consejo de la Unidad.
5. Que en cuanto a la necesidad o no del previo consentimiento informado de los titulares de datos, corresponde indicar que al caso concreto se aplica el artículo 9° literal B) de la Ley N° 18.331, y por ende no resulta necesario recabarlo por tratarse de una Entidad Pública en ejercicio de sus funciones y de una obligación legal.
6. Que por tanto, se encuentran debidamente acreditados todos los requisitos del artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008, para proceder a entregar la información solicitada.

ATENTO: a lo expuesto e informado,

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

DICTAMINA:

1. Indicar que la entrega de la información en la forma solicitada por el Tribunal de lo Contencioso Administrativo se ajusta a las normas de protección de datos personales.
2. NOTIFÍQUESE Y PUBLÍQUESE

MAG. FEDERICO MONTEVERDE

URCDP

Informes

Informe Nº 14/019, de 21 de enero de 2019. Se resuelve una denuncia en relación con la instalación de una cámara de videovigilancia en posible infracción a los requerimientos de protección de datos personales

Informe Nº 16/019, de 22 de enero de 2019. Se resuelve una denuncia referente a la instalación varias cámaras de video vigilancia a través de las que se filma la vía pública y los frentes de las viviendas.

Informe Nº 19/019, de 4 de febrero de 2019. Se resuelve una denuncia referida a la comunicación de datos personales sin consentimiento.

Informe Nº 20/019, de 4 de febrero de 2019. Se informa una consulta realizada por la Unidad Reguladora de Servicios de Comunicaciones, (URSEC) acerca de la legalidad que un operador de televisión para abonados del interior del país, coloque cámaras en la vía pública y transmita en vivo durante las 24 horas a través de su canal local.

Informe N° 30/019, de 7 de febrero de 2019. Se resuelve una denuncia efectuada porque su imagen estaba siendo utilizada por la empresa, sin su consentimiento.

Informe Nº 42/019, de 18 de febrero de 2019. Se resuelve una denuncia referida a la utilización de datos diferentes a los que él había proporcionado.

Informe N° 45/019, de 19 febrero de 2019. Se resuelve una denuncia acerca de la recepción de mensajes de una empresa con la que nunca operó.

Informe N° 54/019, de 25 de febrero de 2019. Se resuelve una denuncia por publicación en Internet de certificados médicos de una trabajadora luego de culminada su relación laboral

Informe Nº 69/019, de 12 de marzo de 2019. Se informa una consulta formulada por el Banco de Previsión Social sobre contestación de oficios judiciales con especial atención a la información referida a montos de prestaciones de actividad y pasividades de afiliados así como otra información de naturaleza sensible.

Informe N° 69/019 bis, de 12 de marzo de 2019. Consulta remitida por la Dirección Nacional de Aduanas con respecto al alcance del artículo 43 de la Ley N° 19.438, de 14 de octubre de 2016, por el que se faculta a esta Dirección a publicar, entre otra, información de nombres de los importadores y exportadores, además de fechas, número de inscripción en el registro aduanero, valor de aduana, país de origen de destino de las mercaderías.

Informe N° 106/019, de 2 de abril de 2019. Se informa una consulta realizada por la Facultad de Veterinaria sobre la posibilidad de grabar los exámenes teóricos tomados en modalidad oral.

Informe Nº 110/019, de 8 de abril de 2019. Se resuelve una denuncia presentada en relación con la instalación de una cámara de video vigilancia en posible infracción a los requerimientos de protección de datos personales.

Informe Nº 111/019, de 8 de abril de 2019. Se informa una consulta presentada por el Banco de Previsión Social respecto a la firma de un Acuerdo de Programa con la organización SMILE TRAIN.

Informe N° 113/019, de 9 de abril de 2019. Se resuelve una denuncia referida al cumplimiento del derecho de supresión.

Informe Nº 184/019, de 27 de junio de 2019. Se informa una consulta realizada por el Instituto de Regulación de Cannabis (IRCCA) sobre el tratamiento correcto a conferir a los datos históricos, teniendo en cuenta que la justicia penal podría solicitar datos sobre personas así como la pertinencia de solicitar autorización para la conservación de datos con fines históricos, estadísticos o científicos.

Informe N° 218/019, de 12 de agosto de 2019. Se resuelve una denuncia referida a la presunta falta de respuesta ante el ejercicio del derecho de acceso.

Informe Nº 276/019, de 30 de agosto de 2019. Se informa una consulta formulada por el Consejo de Educación Técnico Profesional sobre la posibilidad de contar con una base de datos visible en el sitio web de la institución que contenga identificación de las personas (nombre completo, C.I., título obtenido, nivel que se obtiene con él, plan en que cursó y centro educativo), la situación del trámite del título incluyendo la repartición en que se encuentra y fecha.

Informe Nº 281/019, de 2 de setiembre de 2019. Se informa una consulta remitida por la Secretaría Nacional para la lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAF) acerca de la posibilidad legal de esa Secretaría de publicar las resoluciones que imponen sanciones a los sujetos obligados.

Informe Nº 289/019, de 6 de setiembre de 2019. Se informa una consulta formulada por la Dirección Nacional de Empleo del Ministerio de Trabajo y Seguridad Social (DINAE) con respecto al Sistema de Intermediación Laboral y la publicación de información de menores de edad.

Informe Nº 305/019, de 13 de setiembre de 2019. Se informa una consulta presentada por el Colegio Nueva Cultura sobre la

publicación de informaciones vinculadas a denuncias realizadas por madres de alumnos del colegio, a través de páginas web de medios periodísticos nacionales.

Informe S/N, de 24 de setiembre de 2019. Se resuelve analizar un oficio respecto al tratamiento de los datos personales en dos organismos del Estado.

Informe Nº 395/019, de 22 de octubre de 2019. Se resuelve una denuncia sobre el presunto incumplimiento de los plazos para habilitar el ejercicio de los derechos consagrados en la Ley N° 18.331.

Informe Nº 412/019, de 31 de octubre de 2019. Se informa una consulta formulada por la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAFT) respecto a una intimación de entrega de copia de resoluciones que aplican sanciones a los sujetos obligados no financieros remitida por el Tribunal de lo Contencioso Administrativo, a requerimiento de la parte actora en un juicio en que la Secretaría es demandada.

Informe Nº 14/019, de 21 de enero de 2019

Se resuelve una denuncia en relación con la instalación de una cámara de videovigilancia en posible infracción a los requerimientos de protección de datos personales.

Montevideo, 21 de enero de 2019

Exp. 2018-558

Denuncia Patricia Cuello C/ Mercadito Rivera

Informe N° 14

I.- Antecedentes

Con fecha 22 de octubre de 2018, se presentó ante esta Unidad la Sra. AA manifestando que existe una cámara que enfoca hacia la entrada de Rivera 2768 de esta ciudad, lugar donde reside la denunciante, y que la denunciada no posee autorización por parte de la copropiedad para su instalación.

Adjunta nota de la Administración Antoni, fechada en 22 de octubre de 2018, quienes en calidad de administradores del Edificio Obertillo, lugar donde se encuentra instalada la cámara, indican que no hay ninguna Asamblea de Copropietarios en la cual se haya tratado la autorización de la instalación de una cámara de seguridad en la fachada del edificio (fs. 4). Además, adjunta fotos de la ubicación de la cámara (fs. 5).

De la denuncia se procedió a dar vista a Mercadito Rivera, la que fue tomada con fecha 29 de octubre de 2018, y transcurrió el plazo de 10 días hábiles sin evacuar, volviendo el expediente a la informante (fs. 13 a 18)

En virtud de las actuaciones llevadas a cabo, se realizó el Informe N° 438, de 28 de noviembre, por el cual se solicitó dar vista a la Administración Antoni para que ratifique el contenido de la nota y aportara información sobre el propietario del padrón (fs. 19).

La vista fue evacuada por la Administración Antoni, quienes ratificaron lo expresado a fs. 3, en el sentido que el local se encuentra ocupado por el depósito del Mercadito Rivera, desconociendo el contrato existente entre el dueño del padrón y la denunciada. También ratifica lo expresado en cuanto a la inexistencia de Asamblea de Copropietarios que aprobara su instalación (fs. 26)

Posteriormente, se solicitó se requiriera a la Dirección General de Registros, Registro de Comercio, información sobre el titular del padrón, no siendo clara la información de la titularidad arrojada por el Registro.

Con fecha posterior, el expediente volvió para informe jurídico.

II.- Análisis

El presente caso versa sobre la instalación de cámaras de videovigilancia en una propiedad horizontal. En tanto las cámaras tienen la posibilidad de captar imágenes así como sonidos se está ante la presencia de datos personales de conformidad con la definición que a este respecto establece el artículo 4° literal d) de la Ley N° 18.331, de 11 de agosto de 2008. Por tanto, como la citada norma regula todo lo que tiene relación con el derecho a la protección de los datos personales, resulta de plena aplicación al caso concreto.

Sobre este aspecto, el Consejo Ejecutivo de la Unidad mediante Dictamen N° 10/010, de 16 de abril de 2010, definió la videovigilancia como toda grabación, captación, transmisión, conservación y almacenamiento de imágenes, y en algunos casos de sonidos, mediante la utilización de videocámaras u otros medios análogos. Esta norma establece cómo se pueden utilizar sistemas de videovigilancia, qué principios son aplicables y si procede el registro de base de datos personales. También indica los casos en que no es aplicable la normativa de protección de datos, esto es, seguridad pública, defensa del Estado, ejercicio de actividades del Estado en el ámbito penal, cuando se trata del ámbito personal o doméstico de las personas físicas, se utilicen con fines periodísticos o de expresión literaria o artística.

En cuanto a la necesidad de contar con logos de videovigilancia, cabe indicar que su patrón fue aprobado por Resolución de este Consejo N° 989/010, de 30 de julio de 2010.

Es importante expresar que este mismo Dictamen indica que los sistemas de videovigilancia son subsidiarios, y solamente pueden utilizarse cuando no existen otros medios menos lesivos de la intimidad de las personas. Esto es clara aplicación del principio de veracidad regulado en el artículo 7° de la Ley por el cual los datos personales no deben ser *"excesivos en la relación con la finalidad para la cual se hubieren obtenido".* En este sentido, cualquier sistema de videovigilancia que se instale en un determinado ámbito debe respetar este principio y ser idóneo, además debe ser de mínima intervención o afectación a los derechos de las personas.

Por su parte, en la guía de videovigilancia en edificios, complejos y cooperativas de la URCDP, se indica que *"Las cámaras que se utilicen solo podrán enfocar los espacios comunes y que sean considerados de vigilancia necesaria. En el caso de los edificios, se consideran espacios comunes las escaleras, los ascensores, el hall de entrada, los pasillos y cualquier otro determinado por el reglamento de copropiedad, siempre teniendo presente que el número de cámaras no debe ser desproporcionado al área que se vigilará".*

En el presente caso, surge probada la existencia de una cámara instalada en el Edificio Obertillo, que apunta hacia la puerta de entrada del domicilio de la denunciante. Que dicha cámara se presume fue instalada por Mercadito Rivera (Costa y Costa S.A.) en virtud de ser quien tiene alquilado el depósito donde fue instalada la citada cámara.

Además, dicha cámara carece de logos de videovigilancia según la prueba obrante en el presente expediente. Tampoco existe registro en el Sistema de Registros de Bases de Datos Personales con la información captada por la cámara.

A ello se debe agregar, que de conformidad con la información aportada por la Administración Antoni, no existe autorización de la copropiedad para instalar la cámara por parte del Edificio.

Por su parte, de conformidad con el artículo 4° literal k) de la Ley N° 18.331, de 11 de agosto de 2008, el responsable es la persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

Por tanto, en este caso, se presume que es Mercadito Rivera es quien instaló la cámara, y como consecuencia, es responsable por su uso. De acuerdo con el artículo 12 de la citada norma, se debe tener en cuenta que el responsable es responsable por las infracciones a la Ley.

III.- Conclusiones

De conformidad con lo analizado ut supra, se comprueba la existencia de una cámara que apunta hacia la entrada del domicilio de la denunciante, la cual carece de logos identificatorios y de la cual no surge información del Registro de Base de Datos Personales.

También surge probado que dicha cámara no fue instalada de conformidad con lo que establece la normativa de protección de datos, esto es, la cámara no fue instalada con la conformidad de la copropiedad del Edificio.

Que ante el requerimiento de esta Unidad, el Mercadito Rivera no procedió a evacuar la vista conferida a los efectos de que brinde las explicaciones necesarias sobre la instalación de la cámara.

Por tanto, esta informante recomienda que el Consejo Ejecutivo de esta Unidad proceda a la imposición de las sanciones que entienda corresponder, previa vista a la denunciada de conformidad con el artículo 75 del Decreto N° 500/991.

Es todo cuanto tengo que informar.

Dra. Flavia Baladán

Informe Nº 16/019, de 22 de enero de 2019

Se resuelve una denuncia referente a la instalación varias cámaras de video vigilancia a través de las que se filma la vía pública y los frentes de las viviendas.

Montevideo, 23 de enero de 2019

Exp. 2018-296

Denuncia por cámaras de videovigilancia

Informe N° 16

I.- Antecedentes

Con fecha 20 de junio de 2018, el Sr. AA presenta una denuncia ante esta Unidad. En ella indica que en la cuadra donde reside han instalado 8 cámaras de videovigilancia a través de las cuales se filma, además de todo lo que ocurre en la vía pública, los frentes de todas las viviendas. Explica que las cámaras se encuentran cuatro en una cera y cuatro en la otra, filmando cada una hacia la acera del frente, pudiendo filmar incluso lo que sucede en el interior de las viviendas. Agrega que las imágenes son difundidas por Internet a efectos de que algunos vecinos dispongan de las imágenes. Adjunta fotos de las cámaras como medio probatorio (fs. 1 a 19).

El 21 de junio se solicitó averiguar el titular de la dirección denunciada (fs. 22). Con fecha posterior, se procedió a dar vista a los denunciados (fs. 41), cometiéndose ésta por notificación notarial (fs. 57).

La vista fue evacuada con fecha 12 de noviembre de 2018. En sus descargos expresan que la instalación de cámaras es una iniciativa de seguridad promovida por la mayoría de las familias residentes en esa zona de la ciudad. Indican que se trata de una solución tecnológica, de solidaridad vecinal, y de seguridad en la cuadra. Además expresan que cuentan con un grupo de Whatsapp, cartelería de vecinos en alerta, reuniones de análisis de proyectos, todo ello con la finalidad de combatir la inseguridad. Indican que las cámaras fueron financiadas en forma colaborativa por los vecinos y la instalación estuvo a cargo de ellos mismos. Expresan que están en contacto con el Ministerio del Interior a efectos de iniciar acciones colectivas. Por último, dicen que ante el reclamo concreto, han implementado una prestación del sistema por medio de la cual se bloquea la visión de una zona de la logrando evitar la captación de imágenes de la vivienda del denunciante. Adjuntan imagen actual de la cámara y carta firmada por los vecinos que aceptan la instalación de este sistema (fs. 61 a 66).

De los descargos presentados, se procedió a dar vista al denunciante para que expresara su conformidad con la solución propuesta por los denunciados así como todo otro elemento que considere correspondiera al caso (67). La vista fue evacuada por el denunciante, quien expresó que no posee control sobre las imágenes, por lo que se ve impedido de corroborar las imágenes registradas. Que previo a la denuncia ya se le había expresado que su vivienda no iba a ser captada por las imágenes, no siendo así en los hechos. Que el hecho que presenta el acto de filmar y registrar todo lo que ocurre en la vía pública es ilegítimo y por último que la carta es firmada por 25 de por lo menos 37 vecinos que viven en la cuadra.

En forma complementaria, se procedió a dar vista al Ministerio del Interior, específicamente a la Dirección General de Fiscalización de Empresas, a los efectos de que se exprese sobre los extremos allí indicados. Esta Entidad indicó que la Dirección General no habilita cámaras ni sistemas de cámaras (sean individuales o barriales) así como tampoco está a su cargo el contralor de la disposición de las cámaras de seguridad, los registros fílmicos, etc. Aclaran que la instalación doméstica no está dentro del contralor de esta Dirección por lo que no se requeriría que este grupo vecinal habilite el sistema (fs. 81 a 82). Posteriormente, el expediente pasó para informe jurídico.

II.- Análisis

El presente caso versa sobre un tema de videovigilancia, específicamente sobre la legitimidad de colocar un sistema de videovigilancia en acuerdo entre personas físicas a los efectos de vigilar lo que sucede en una determinada zona de la ciudad de Montevideo.

En tanto las cámaras tienen la posibilidad de captar imágenes así como sonidos se está ante la presencia de datos personales de conformidad con la definición que a este respecto establece el artículo 4° literal d) de la Ley N° 18.331, de 11 de agosto de 2008. Por tanto, como la citada norma regula todo lo que tiene relación con el derecho a la protección de los datos personales, resulta de plena aplicación al caso concreto.

Sobre este aspecto, el Consejo Ejecutivo de la Unidad mediante Dictamen N° 10/010, de 16 de abril de 2010, definió la videovigilancia como toda grabación, captación, transmisión, conservación y almacenamiento de imágenes, y en algunos casos de sonidos, mediante la utilización de videocámaras u otros medios análogos. Esta norma establece cómo se pueden utilizar sistemas de videovigilancia, qué principios son aplicables y si procede el registro de base de datos personales. También indica los casos en que no es aplicable la normativa de protección de datos, esto es, seguridad pública, defensa del Estado, ejercicio de actividades del Estado en el ámbito penal, cuando se trata del ámbito personal o doméstico de las personas físicas, o

cuando se utilicen con fines periodísticos o de expresión literaria o artística. Es importante expresar que este mismo Dictamen indica que los sistemas de videovigilancia son subsidiarios, y solamente pueden utilizarse cuando no existen otros medios menos lesivos de la intimidad de las personas.

En cuanto a la necesidad de contar con logos de videovigilancia, cabe indicar que su patrón fue aprobado por Resolución de este Consejo N° 989/010, de 30 de julio de 2010.

En el presente caso, cabe dilucidar si es adecuado a la normativa de protección de datos personales, la instalación de cámaras que captan parte de la vía púbica fundados en razones de seguridad.

A este respecto cabe expresar que la función de seguridad de los espacios públicos corresponde en exclusividad al Ministerio del Interior, en ejercicio de sus competencias de velar por la seguridad pública. En ese marco, es necesario determinar que se considera por vía pública. Según el Diccionario de la Real Academia Español ésta se define como *"f. Calle, plaza, camino u otro sitio por donde transita o circula el público".* Sobre este punto la Agencia Española de Protección de Datos en su Resolución R/02340/2012 se remite a la definición citada a la cual agrega que "…*debe insistirse en que la titularidad privada de un terreno abierto no justifica per se la realización de grabaciones de imágenes en el caso de que se trate de un "lugar público".*

A ese respecto además es necesario indicar que en determinados casos resulta imprescindible captar parte de la vía pública para la finalidad de vigilancia que se pretende realizar, como por ejemplo sucede con las cámaras puestas en las porterías de los edificios. Ahora bien, no por ello se puede interpretar que ello habilita a captar la vía pública.

A efectos de profundizar en este aspecto debe recordarse la aplicabilidad del principio de veracidad, regulado en el artículo 8° de la Ley N° 18.331, de 11 de agosto de 2008, por el cual se indica que los datos personales que se recaben deben ser *"… adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido"*. Esto es lo que se denomina en la doctrina "*proporcionalidad"* y es el criterio que debe tenerse en cuenta a la hora de instalar cámaras de videovigilancia.

No debe olvidarse además que con la intención de lograr mayor seguridad, se pueden llegar a adoptar medidas restrictivas de derechos fundamentales como lo es el derecho a la intimidad, el cual es restringido por la existencia de sistemas de videovigilancia.

Por tanto, esta informante entiende que la videovigilancia debe ser una medida adecuada, pertinente y no excesiva en relación con la finalidad perseguida y que se debe justificar la instalación de cámaras de vigilancia. Además, se debe analizar si la finalidad de seguridad no puede alcanzarse por otros medios alternativos, menos intrusivos para el derecho a la protección de datos personales.

III.- Conclusiones

En virtud de lo analizado, esta informante entiende que en el caso se deben adoptar todas las medidas necesarias para no captar de ninguna forma imágenes relacionadas con la vivienda del denunciante, no siendo suficiente la solución planteada al no poder el denunciante controlar su funcionamiento.

Asimismo, se considera que los vecinos que deseen compartir imágenes de sus casas están en su derecho, no pudiendo captar la vía pública más allá de lo mínimo imprescindible.

Además, si las cámaras graban, se debe proceder a inscribir las bases de datos y a indicar la existencia de cámaras con los logos recomendados por esta Unidad a los efectos de que las personas que puedan sentir vulnerado su derecho a la protección de datos puedan ejercer sus derechos, tal como lo establece la Ley N° 18.331, de 11 de agosto de 2008.

Es todo cuanto tengo que informar.

Dra. Flavia Baladán

Informe Nº 19/019, de 4 de febrero de 2019

Se resuelve una denuncia referida a la comunicación de datos personales sin consentimiento.

Informe Nº 19

Montevideo, 04 de febrero de 2019

Exp. 2018-2-10-0000349

Ref. Denuncia Sr. AA contra escuela Brother por correo electrónico

I. Antecedentes

I. La presente viene a consideración de la Unidad Reguladora y de Control de Datos Personales (URCDP), en virtud de la denuncia formulada por el señor AA contra Escuela Brother, por presunto incumplimiento de la Ley N° 18.331 de 11 de agosto de 2008.

II. Expresa el denunciante que recibió un correo electrónico invitándole a completar un formulario de un Plan de Marketing de la Escuela, el cual se envió "en forma masiva y con todas las direcciones visibles para todos".

III. Según consta a fojas 17 del expediente se dio vista a Mauricio Pablo Suarez Rassinetti (Escuela Brother), quien se presentó escrito a fojas 21 y siguientes.

IV. A fojas 44 y 45, las señoras María Fernanda Gómez y Valentina Andrea Clavero tomaron vista de las presentes actuaciones presentando escrito a fojas 49 y siguientes.

II. ANALISIS

I. <u>De la actuación de Mauricio Pablo Suarez Rassinetti (Escuela Brother</u>): Surge del escrito presentado por la denunciada que con fecha 29 de mayo de 2018 dos estudiantes de la Escuela Técnica Superior de Administración y Servicios de la Universidad del Trabajo del Uruguay, señoras María Fernanda Gómez y Valentina Andrea Clavero, "fueron autorizadas a acceder a información de Brother únicamente con fines EDUCATIVOS y a los solos efectos de aprendizaje (...)". Indica además en el punto 5 del escrito que "las estudiantes no son alumnas de la ESCUELA BROTHER y no tienen relación alguna con la institución".

II. Agregan en el punto 6 del escrito que, a los efectos de dar cumplimiento a los artículos 10, 11 y 12 de la Ley N° 18.331 de 11 de agosto de 2008, suscribieron con las estudiantes un acuerdo de confidencialidad "en el cual las estudiantes se obligaron a no difundir información". Aportan copia del acuerdo (fs. 30).

III. Por otra parte manifiestan que "las estudiantes fueron quienes difundieron la información y enviaron el mail, incumpliendo el acuerdo de confidencialidad suscrito y violando la Ley 18.331(...)"

IV. Corresponde señalar que la escuela Brother es la responsable de la base de datos o del tratamiento, pues es la propietaria de la base o decide sobre la finalidad, contenido y uso del tratamiento. Por tanto, son de aplicación al caso concreto los artículos 6°, 8°, 10, 11, 12 y 17 de la citada Ley.

V. El correo electrónico que recibió el denunciante identificaba a la Escuela Brother, único responsable desde el punto de vista de la protección de datos por aplicación del artículo 12. En este sentido, se verifica una vulneración del principio de finalidad (art. 8°) pues los datos objeto de tratamiento "no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención", lo que ocurrió en el caso concreto.

VI. Además, en el accionar de Brother se verifica un incumplimiento del artículo 17 de la Ley dado 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, (subrayado dela informante) al que se le debe informar sobre la

finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo". Claramente dichos extremos no fueron respetados por la denunciada al efectuar la comunicación sin el consentimiento del titular del dato ni encuadra dentro de las excepciones previstas en los literales A, B y C del mismo artículo 3 siendo suficiente para deslindar de responsabilidades a la empresa Brother el acuerdo suscrito con las estudiantes.

VII. Expresa Brother en el punto 9 de su escrito que "no solicitó el consentimiento informado porque el caso encuadraba como una excepción a los artículos 8 y 9 (…)" pues no se requiere el consentimiento cuando se trate de "listados cuyos datos se limiten (…)". Respecto a este punto debe señalarse que la excepción prevista en el artículo 9 literal C), es de interpretación estricta, por lo que el consentimiento no se encuentra exceptuado para otros datos que no se encuentren en la enumeración taxativa, (en el caso el correo electrónico no forma parte del listado previsto por el artículo citado).

VIII. Por último, corresponde señalar que no surge registro de base de datos a nombre de la empresa Brother (RUT 214803800013), o a nombre del Sr. Mauricio Pablo Suarez Rassinetti, existiendo por tanto además contravención de lo establecido en el artículo 6° de la Ley citada.

IX. De la actuación de las señoras María Fernanda Gómez y Valentina Andrea Clavero: Surge del escrito presentado a fojas 49 y siguientes que se trata de dos estudiantes de la Tecnicatura de Analista en Marketing de la escuela Técnica Superior de Administración y Servicios de la Universidad del Trabajo del Uruguay. Indican que cometieron el error de enviar la encuesta "sin haber seleccionado la opción copia oculta" con todas las direcciones de correo electrónico a la vista.
La conducta señalada encuadra en el incumplimiento del artículo 17 de la citada Ley, habiendo divulgado y comunicado los correos electrónicos sin el consentimiento del titular del dato.

III. Conclusiones

I. En virtud del análisis efectuado, corresponde señalar que la empresa Mauricio Pablo Suarez Rassinetti (Escuela Brother) ha incumplido con las disposiciones de la Ley N° 18.331 de 11 de agosto de 2008, en particular los artículos 6°, 8°, 10, 11, 12 y 17, en cuanto:

- no ha garantizado en forma suficiente la seguridad y confidencialidad de los datos personales comunicando los datos personales sin el consentimiento del titular del dato y fuera de las hipótesis previstas en los literales A, B y C del artículo 17.

- no ha inscripto sus bases de datos.

II. En cuanto a las señoras María Fernanda Gómez y Valentina Andrea Clavero se verifica un incumplimiento del artículo 17 de la Ley citada.

III. Por lo anterior, se sugiere la aplicación de las sanciones que el Consejo Ejecutivo de la URCDP estime convenientes a Mauricio Pablo Suarez Rassinetti (Escuela Brother) y las señoras María Fernanda Gómez y Valentina Andrea Clavero.

IV. Se sugiere intimar a Mauricio Pablo Suarez Rassinetti (Escuela Brother) la inscripción de las bases de datos que correspondan en un plazo de 30 días corridos bajo apercibimiento de ulteriores sanciones.

V. Antes de la aplicación de la sanción, se sugiere previa vista conforme al artículo 76 del Decreto 500/91.

Dra. María Cecilia Montaña Charle

Derechos Ciudadanos

Informe Nº 20/019, de 4 de febrero de 2019

Se informa una consulta realizada por la Unidad Reguladora de Servicios de Comunicaciones, (URSEC) acerca de la legalidad que un operador de televisión para abonados del interior del país, coloque cámaras en la vía pública y transmita en vivo durante las 24 horas a través de su canal local.

Montevideo, 04 de febrero de 2019

Ref. Expediente 2019-2-10-0000002 Consulta realizada por URSEC referente a la legalidad de la colocación de cámaras en la vía pública. (San Ramón)

Informe N° 20

I.-Antecedentes

La presente viene a consideración de esta Unidad en función de la consulta remitida por el Dr. Gustavo Sorrentino, Secretario General de la Unidad Reguladora de Servicios de Comunicaciones (URSEC) por la cual solicita que el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP), emita dictamen "en los términos del Art. 34, literales A y F de la Ley 18.331 de 11 de agosto de 2008".

Específicamente el consultante solicita dictamen en referencia a la consulta realizada por la Sra. AA, la que expresa:

"Estimados de URSEC buenos días, Agradezco me puedan informar si es legal que un operador de televisión para abonados del interior del país coloque cámaras en la vía pública y trasmita en vivo durante las 24 horas a través de su canal local, todo lo que capta con sus cámaras. Algunos habitantes de la localidad consideramos que esa operativa invade el derecho a la privacidad e incluso entendemos que afecta el derecho a la protección de imagen. Esto está sucediendo en la Localidad de San Ramón, Dpto. de Canelones, el operador comercial de TV para abonados es la empresa TINTAGE SA Cable satelital de San Ramón, Rut 21445 502 0011".

I.-Análisis y marco jurídico de aplicación

Respecto a la consulta planteada corresponde indicar que conforme al artículo 4° literal D) de la Ley número 18.331 de 11 de agosto de 2008 (LPDP), dato personal es toda información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. Por tanto, la imagen encuadra en la mencionada definición.

En este sentido el Consejo Ejecutivo de la URCDP se ha pronunciado anteriormente indicando que "La imagen de las personas es un dato personal y, como tal, su tratamiento debe ajustarse a los parámetros legales" (Principales criterios de la Unidad Reguladora y de Control de Datos Personales (2009 – 2015). Agrega en el Dictamen N° 10/010, de 16 de abril de 2010 que la videovigilancia "es toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo y esas imágenes constituyen información personal y por tanto será de aplicación la LPDP y sus normas complementarias."

En el caso que nos convoca, debemos determinar si corresponde o no la colocación de cámaras que captan imágenes de la vía pública por parte de un operador de televisión para abonados del interior, para su difusión a través del canal de cable. Debe tomarse en cuenta que, conforme a la definición antes señalada, la sola reproducción en tiempo real de imágenes captadas por las cámaras supone un tratamiento de datos personales como viene de señalarse, entendida este como "cualquier 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" (art. 4° literal M de LPDP).

Debemos tener presente que la actuación de los individuos se encuentra regida por el principio de libertad consagrado en el artículo 7° y 10 de la Constitución de la República, por el cual la única limitación al ejercicio de los derechos (vida, honor, libertad, seguridad, trabajo y propiedad) estará dada por leyes que se establezcan

por razones de interés general. Ningún habitante de la República será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.

En este sentido, la limitación a la colocación de las cámaras está dada por los requisitos que han sido establecidas por la LPDP, en especial sus principios.

No caben dudas que la colocación de cámaras de videovigilancia con fines de seguridad pública está atribuida al Ministerio del Interior, y en el caso de contralor del tránsito y policía de espacios públicos, a los Gobiernos Departamentales específicamente dentro de las funciones del Intendente, conforme al art. 35, numeral 25 la Ley N° 9.515, en cuanto a la organización y cuidado de la vialidad pública, la que puede ser ejercida mediante la colocación de cámaras (Dictamen N° 15/018, de 04 de setiembre de 2018).

Ahora bien, la colocación de cámaras por particulares en la vía pública tiene los límites establecidos por la LPDP a saber, la actuación de los responsables de las bases de datos debe ajustarse a los principios generales conforme a lo establecido en el artículo 5° (Legalidad, Veracidad, Finalidad, Previo consentimiento informado, Seguridad de los datos, Reserva y Responsabilidad). Asimismo, el artículo 6° indica que "la formación de la bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia.

Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes (…)". Al tenor del artículo 7° "los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad (subrayado de la informante)".

En aplicación de los precitados artículos puede interpretarse que no podrán colocarse de cámaras en espacios públicos si captan lugares, personas, matrículas, números de puerta u otro dato similar que identifique o haga identificable a una persona si no se da cumplimiento a la obtención del consentimiento previo, expreso e informado (art 9° y 13 LPDP). Más aun tomando en cuenta que la retrasmisión de las imágenes configura una hipótesis de comunicación de datos en los términos establecidos en el artículo 17 de la Ley citada.

Sobre este punto se entiende por comunicación de datos "toda revelación de datos realizada a una persona distinta del titular de los datos" (art. 4° literal B de LPDP).

III.-Conclusiones

Desde el punto de vista de la protección de datos personales, la colocación de cámaras en la vía pública solo es posible si se da cumplimiento a los principios rectores en la materia.

En este sentido, si las cámaras se colocan en lugares que capten en forma general la ciudad o son de baja resolución (se aplican filtros de privacidad), y no permiten la identificación de las personas, no existe limitante.

No obstante, si las cámaras están orientadas a lugares privados y permiten la identificación de las personas, deberá cumplirse con los requisitos establecidos en la Ley, (obtención del consentimiento previo, expreso e informado, inscripción de la base de datos) o deberán ser retiradas por incumplimiento del principio de legalidad.

Es todo cuanto tengo que informar.

Dra. María Cecilia Montaña Charle

Derechos Ciudadanos

Informe Nº 30/019, de 7 de febrero de 2019

Montevideo, 07 de febrero de 2019

Exp. 2018-2-10-0000543

Ref. Denuncia Sr. AA contra empresa Eeasy Go por publicación de imagen sin consentimiento del titular.

Informe Nº 30

I.- Antecedentes

I. La presente viene a consideración de la Unidad Reguladora y de Control de Datos Personales (URCDP), en virtud de la denuncia formulada por el señor AA contra Easy Go (Easy Taxi SA), por presunto incumplimiento de la Ley N° 18.331 de 11 de agosto de 2008.

II. Expresa el denunciante que “tomé conocimiento de que mi imagen estaba siendo utilizada por la empresa, sin mi conocimiento, permiso, ni autorización para promocionar sus servicios en las Redes Sociales a través de "Historias" que son generadas por la Sra. BB durante sus viajes”.

III. Agrega además que “La Sra. BB tiene un acuerdo con dicha empresa, por el cual a cambio de generar las "Historias" obtiene viajes gratis”. Aporta captura de pantalla de una historia de Instagram (fs. 6).

IV. Según consta a fojas 13 del expediente se dio vista a Easy Go (Easy Taxi SA), quien se presentó escrito a fojas 19.

II.- Análisis de los hechos

I. En el escrito presentado manifiesta la denunciada que “Easy SA no difundió ni utilizó de forma alguna, imágenes del Sr. AA habiéndolo hecho en todo caso un tercero”. Agrega que si algún tercero difundió las imágenes “fue por su cuenta y riesgo y no en representación ni en cumplimiento de algún contrato mantenido con esta empresa”. Continúa diciendo que no tiene ningún contrato o acuerdo que implique para su cumplimiento difusión de imágenes de conductores. Por último desconocen la captura de pantalla indicando que “carecen de cualquier tipo de autenticidad (...)”.

II. Atento a los descargos presentados se dio vista a la parte denunciante a los efectos de que proporcionara datos de contacto de la Sra. BB, lo cual realizó a fs. 31. Asimismo reitera que las imágenes aportadas son auténticas sin embargo habiendo sido controvertidas por la denunciada no las presentó nuevamente con los recaudos necesarios, entiéndase, certificadas notarialmente. Por tanto dicha prueba no será admisible tomando en cuenta lo establecido en el artículo 70 del Decreto 500/991.

III. El Sr. AA agrega en el punto c) de su escrito que mantuvieron reunión con la empresa Easy Go el 27 de setiembre de 2018 con la Sra. Adriana Vicuña Manager Operations de Easy Uruguay, la que le informó “en forma presencial, personal y directa” que la empresa tenía un contrato con la Sra. BB para la generación de “Historias” a partir de los viajes que ésta realizaba en los vehículos particulares que utilizaban la aplicación informática (...)”. Indica además a partir de lo ocurrido “el acuerdo con la Sra. BB había sido suspendido”.

IV. Atendiendo a la discordancia entre los dichos de ambas partes, se convocó a audiencia de testigos a la Sra. Adriana Vicuña, según lo solicitado por la denunciante. Se citó audiencia de prueba testimonial para el día Miércoles 19 de diciembre a las 10.00 hs. y se solicitó se diera vista a la Sra. BB.

V. Durante la realización de la audiencia de prueba testimonial la empresa Easy Taxi SA informa que la Sra. Adriana Carolina Vicuña Parra fue dada de baja de la empresa con fecha 6 de diciembre de 2018, aportando la constancia respectiva emitida por el Banco de Previsión Social. Asimismo informa que la incomparecencia de la testigo se debe a que no se encuentra en el país.

VI. En escrito presentado a fojas 52 comparece la Sra. BB, representada por sus padres en ejercicio de la patria potestad que “no existe entre la Sra. BB y la empresa Easy Taxi S.A. contrato de ningún tipo, razón

por la cual resulta imposible presentar lo solicitado en la vista".

VII. De los puntos antes detallados no surge probado incumplimiento de la normativa de protección de datos personales, no resultando acreditado en debida forma la utilización de imágenes que identifiquen o hagan identificable al Sr. AA, en los términos del artículo 4 literal D) de la Ley N° 18.331 de 11 de agosto de 2011 (LPDP). Tampoco resulta acreditado (en el caso de admitirse que la imagen sí pertenezca al Sr. AA), que la publicación haya sido realizada por la empresa Easy Taxi SA (ni por si ni por interpuesta persona), careciendo de legitimación pasiva, no habiéndose comprobado relación contractual con la Sra. BB.

III.- Conclusiones

I. Corresponde señalar que desde el punto de vista de la Protección de Datos Personales no surge probado en el expediente que la empresa Easy Taxi SA (Easy GO) haya realizado comunicación de datos sin el consentimiento del titular en los términos del artículo 17 de la LPDP ni por si ni por interpuesta persona.

II. No surge debidamente acreditado que la publicación de la "Historia" en Instagram pertenezca al Sr. AA, no habiéndose presentado el material probatorio en forma.

III. No surge probada relación contractual entre la Sra. BB y la empresa Easy Taxi SA (Easy GO).

IV. En virtud de lo anterior, se sugiere el archivo de las presentes actuaciones por no verificarse contravención a las disposiciones de la mencionada ley.

V. Previo al archivo de las presentes actuaciones se sugiere, vista conforme al artículo 75 del Decreto 500/91.

Dra. María Cecilia Montaña Charle

Derechos Ciudadanos

Informe N° 45/019, de 19 febrero de 2019

Se resuelve una denuncia acerca de la recepción de mensajes de una empresa con la que nunca operó.

Montevideo, 19 de febrero de 2019

Exp. 2018-2-10-0000572

Ref. Denuncia Sra. AA Cabrera contra Telefónica Móviles del Uruguay S.A. por comunicación de datos sin consentimiento.

Informe Nº 45

Antecedentes

I.-

El presente viene a consideración de la Unidad Reguladora y de Control de Datos Personales (URCDP), en virtud de la denuncia formulada por la Sra. AA contra Telefónica Móviles del Uruguay SA (Movistar).

Expresa la denunciante que el 25 junio de 2018 recibió en su domicilio una notificación de Equifax-Clearing de informes, por la que se le comunica que se procedió a registrarla en la base de datos por una obligación incumplida, que mantendría con Movistar por un monto de $24.450. Agrega “nunca he celebrado contrato con la denunciada, por lo que, en varias oportunidades me comunique a fin de que se le informara el origen de la deuda y cómo se habrían obtenido mis datos personales”.

Agrega la denunciante que ante la falta de información se presentó ante el Área de Defensa del Consumidor para solicitar la exclusión del Clearing, situación que se concretó el 04 de setiembre de 2018.

Indica además, que el 22 de octubre de 2018 recibe nuevamente carta de Clearing, en la que se procedió a su registro en la base de datos por una supuesta deuda con Movistar. La Sra. AA expresa que nunca prestó su consentimiento informado para que el responsable de la base de datos obtenga y comunique a terceras personas sus datos personales.

Aporta cartas de Equifax-Clearing de informes recibidas el 25 de junio y el 22 de octubre de 2018; reclamo realizado ante el Área de 21 de setiembre de la cual surge que le solicita realice la denuncia policial y presente carta de desconocimiento de la línea telefónica.

A fojas 17 agrega constancia de reclamación formulada en el Área de Defensa del Consumidor el 31 de octubre de 2018 ante la segunda carta recibida de Clearing. En la reclamación agrega que “Al día de hoy no le informan si existió la comunicación telefónica de aceptación de la contratación y continúan enviando dicha comunicación de clearing”.

II.-

Se confirió vista a Telefónica Móviles del Uruguay SA (Movistar), quien con fecha 10 de diciembre de 2018 presenta escrito de evacuación que luce a fojas 29 y siguientes. Expresa que “la Sra. Cabrera presentó su reclamo en el Área de Defensa del Consumidor, el cual quedó resuelto habiéndose efectuado los ajustes correspondientes y su exclusión del Clearing si antecedentes, como surge a fs. 17 de estos autos, adjuntada por la propia Sra. AA”.

En cuanto a lo expresado a fojas 17, el Área de Defensa del Consumidor indica ante el reclamo de la Sra. AA (Fs. 17) que “Se realiza gestión con la empresa Telefónica Móviles del Uruguay SA, en fecha 26/10/2018, la que responde lo siguiente: Estimados. En referencia a este reclamo, por un error del sistema, los ajustes en la cuenta se procesaron tarde, Y por ello no había quedado excluido del clearing de informes sin antecedentes. Al día de hoy, ya quedaron procesados los ajustes en la cuenta del cliente y procesada correctamente la exclusión

del clearing sin antecedentes". Cabe enfatizar que según expresa la Sra. AA, no es cliente de Movistar, por lo que no correspondería que se realicen ajustes "en la cuenta del cliente".

Manifiesta Movistar que no trasgredió la Ley N° 18.331 en cuanto la información que entrega a Equifax-Clearing de informes "se limita al nombre, apellido, cédula de identidad y domicilio. Todos ellos datos para los cuales no es necesario recabar el consentimiento previo, según lo establece expresamente el art. 9 de la Ley 18.331: "… 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…"

Agrega Movistar que "En cuanto al tratamiento de los mismos (…) "Queda expresamente autorizado el tratamiento de datos destinado a informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor o en las circunstancias previstas en la presente ley".

Por último, Movistar cita el Dictamen 5/2011 de la Unidad, en cuanto a la procedencia de inscripción de una deuda en base de datos de Clearing de Informes. Analizado el dictamen de referencia, puede apreciarse que no es de aplicación al caso concreto puesto que se consulta sobre la procedencia de la inscripción de una deuda en la base de datos de Clearing de Informes, así como de los medios legales de que dispone para la defensa de sus derechos, al amparo de lo previsto por el articulo 34 lit. A de la Ley N° 18.331.

III.-

En cuanto a los puntos antes señalados, corresponde efectuar las siguientes precisiones. Conforme al precitado artículo 9° literal C), no se requiere el consentimiento previo para el tratamiento de datos cuando la información se encuentre contenida en listados "cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento". Si el listado contiene algún otro dato, será necesario el consentimiento, siendo de interpretación estricta, por tanto, al Clearing de Informes se comunican no solamente "nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento" sino además que es cliente de Movistar (lo cual en el caso no se ajusta a la realidad), y el monto del adeudo.

Respecto al artículo 22 antes citado, autoriza la formación de los llamados Bureau de crédito, aplicable en el caso al tratamiento que realiza Equifax-Clearing de Informes y no a Movistar. Si esta última empresa ha comenzado a formar este tipo de bases de datos (destinadas a informar sobre la solvencia patrimonial o 4 crediticia…), deberá inscribirla ante la Unidad, de conformidad con el artículo 6° de la citada Ley.

IV.-

Expresa Equifax Uruguay SA a fs. 39 que de la Base de datos de Equifax no surge ningún incumplimiento registrado a nombre de la Sra. AA. Aportan copia del informe comercial de la denunciante en tal sentido.

Agrega que en los casos en que se envían cartas comunicando el registro de operaciones incumplidas en la base de datos (fs. 41), "Equifax actúa siempre a solicitud expresa de sus afiliados, bajo sus instrucciones específicas y en el marco de un contrato vigente (…)" Indica que es el propio acreedor de la deuda quien indica qué comunicaciones realizar, su contenido y a quien se envía.

Por lo anterior, no se verifica incumplimiento de la normativa de protección de datos personales por parte de Equifax Uruguay SA.

V.- Análisis

La denuncia planteada en estos obrados versa sobre la adjudicación de una línea telefónica a una persona sin

demostrar las medidas que fueron adoptadas por la empresa a los efectos de verificar la identidad de la contratante. Es de suma importancia tener en cuenta, que no fueron aportadas las grabaciones en las que se perfecciona el contrato, aun siendo solicitadas por la denunciante en el Área de Defensa del Consumidor en varias oportunidades.

Es de aplicación al caso concreto la Ley N° 18.331, de 11 de agosto de 2008, su normativa complementaria y modificativa, dado que estamos ante la presencia de datos personales en tanto se trata de información que identifica a una persona (art. 4° literal d).

En este sentido verifican una vulneración al principio de veracidad estatuido en el artículo 7° de la citada Ley en tanto los datos que se recolecta Movistar a los efectos de su tratamiento deben ser veraces y en caso de constatarse la inexactitud o falsedad de los datos (lo que se reclama en más de una oportunidad por parte de la Sra. AA), el responsable del tratamiento deberá suprimirlos, (o sustituirlos o completarlos según el caso). Ello debido a que no existe prueba de que se haya verificado la identidad de la persona (no se aporta contrato firmado ni grabación), es decir se le adjudicó la línea sin verificar la identidad y por ende se incumple además el artículo 9° de la Ley (previo consentimiento informado).

Por otra parte, Movistar aduce “un error del sistema” para justificar la nueva comunicación de los datos de la Sra. AA a Equifax, sin aportar prueba alguna de sus dichos, dejando en evidencia el incumplimiento de lo preceptuado en el artículo 10 de la Ley relativo al Principio de seguridad de los datos, por cuanto deben adoptarse las medidas que “resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado (…)”.

Por último corresponde señalar que, una vez que se ha solicitado por parte de la Sra. AA la supresión de sus datos, “El responsable de la base de datos o del tratamiento deberá proceder a realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato”, según lo preceptuado en el artículo 15 de la Ley. En el caso se verifica un incumplimiento en este sentido por parte de Movistar.

VI.- Conclusiones

De los puntos antes mencionados corresponde enfatizar:

1.- Se verifica un incumplimiento de los artículos 7°, 10 y 15 de la Ley N° 18.331 por lo que se recomienda la aplicación de las sanciones que el Consejo Ejecutivo estime convenientes.

2.- Se sugiere al Consejo Ejecutivo exhorte a Telefónica Móviles del Uruguay SA (Movistar) ajuste los procedimientos internos a fin de que quienes contraten servicios con la empresa acrediten su identidad fehacientemente y para que, recibida una solicitud de acceso, rectificación, actualización, inclusión o supresión se dé cumplimiento a los plazos establecidos en los artículos 14 y 15 de la citada Ley a los efectos de evitar en un futuro situaciones similares.

3.- Se solicita se de vista en los términos del artículo 76 del decreto 500/991 a la denunciada.

Es todo cuanto tengo que informar.

Dra. María Cecilia Montaña Charle

Derechos Ciudadanos

Informe Nº 42/019, de 18 de febrero de 2019

Se resuelve una denuncia referida a la utilización de datos diferentes a los que él había proporcionado.

Montevideo, 18 de febrero de 2019.

Expediente N° 2018-2-10-0000772.

Denuncia Sr. AA contra Tienda Inglesa y Banco Scotiabank por utilización de datos sin consentimiento

Informe jurídico Nº 42

I. Antecedentes

Con fecha 20 de diciembre de 2018 presenta ante la Unidad Reguladora y de Control de Datos Personales (URCDP), el Sr. AA una denuncia contra Tienda Inglesa y Banco Scotiabank Uruguay (en adelante (Scotiabank), por utilización de datos sin consentimiento.

El denunciante solicita se inicien las actuaciones correspondientes por la Unidad. Así se procede a dar vista de estos obrados a través de telegrama colacionado a los denunciados, quienes comparecen a tomar la vista respectiva y a presentar sus aclaraciones.

II. Argumentos de las partes

El denunciante manifiesta que obtuvo una tarjeta de débito a través de Tienda Inglesa, declarando su domicilio real. Cuando le llega la tarjeta, la recibe y luego de unos días se da cuenta que en la hoja que trae la tarjeta figura su nombre y domicilio que nunca dio al Scotiabank (banco que emite la tarjeta), ni a ningún de los bancos anteriores que derivaron en este.

Ejerce su derecho de acceso ante el Scotiabank y no le han contestado habiendo pasado el tiempo legal (adjunta documentación, fojas 1 a 5).

Los denunciados son Tienda Inglesa y Scotiabank Uruguay S.A., los que tomaron vista y se notificaron.

La primera se presenta y manifiesta que: el denunciante indicó como su domicilio la calle XX 1111 apto 111, lo que fue verificado con la constancia de domicilio presentada por este, dato que fue transmitido al banco para la realización de la tarjeta de débito, y no la dirección que surge al momento de ser esta entregada en el domicilio del denunciante (foja 33).

El segundo aclara que: llega a su conocimiento esta denuncia al momento de ser notificados, momento en el que comienzan a verificar los hechos mencionados en ella. De esa verificación surge que:

a) Una vez verificados los hechos surge que el domicilio que el denunciante indica no haber proporcionado surge de la base de datos de clientes de la institución desde el año 2007, ya que fue proporcionado por quién era su esposa en ese momento. El sistema del banco toma los datos registrados, en este caso el domicilio de la calle XXX 1111. Ese dato le fue proporcionado al banco en 2007 por su cónyuge. Actualmente se procedió a la actualización del dato (foja 16).

b) En cuanto a la entrega en tiempo y forma de la información solicitada por el denunciante el plazo fue cumplido efectivamente desde el banco pero existió una demora interna del procedimiento de envío del correo electrónico, el que fue enviado el lunes y no el martes como debía ser (foja 17).

III. Análisis de la denuncia

En primer término se entiende que Tienda Inglesa ha comunicado los datos en concordancia con lo informado por el denunciante. Su domicilio real, de acuerdo con sus declaraciones en el momento de estos obrados es la dirección proporcionada por él (XXXX 1111 apto 111) lo que además queda de manifiesto en la documentación presentada por Scotiabank (foja 21).

En segundo lugar Scotiabank tiene una base de datos de clientes con información del año 2007, año en el que la Ley de Protección de Datos no había sido promulgada todavía. A partir del 11 de agosto de 2008 fue promulgada la Ley N° 18.331 de Protección de Datos y Acción de Habeas Data, por lo que comienza a regir para todas las bases de datos que contienen datos personales, como la base de clientes del banco. Base de datos utilizada para verificar si una persona es cliente o no del banco.

En este caso el denunciante no es cliente del banco sino que indirectamente se encuentra su nombre en la base, porque en el año 2007 su cónyuge en ese momento lo declaró como tal.

Esta información forma parte de los datos solicitados a su cónyuge en el momento que esta opera con el banco (cónyuge, domicilio XXX 111), no para que sea utilizada para otra persona por más que en ese entonces fuera su cónyuge. Los datos personales son información de cada persona (artículo 4° de la Ley N° 18.331), actuando para cada uno en forma independiente no en conjunto, por lo que no se debe dar por entendido que los datos contenidos en la base de datos, como en este caso, se pueden utilizar para otra persona, aunque sea su cónyuge, como sucedió según lo que surge de los dichos del propio banco (fojas 16 y 17).

En cuanto al incumplimiento del plazo mencionado en el artículo 14, es necesario que se adecuen los tiempos para que los correos salgan en tiempo y forma y no verse perjudicados.

En relación con lo mencionado anteriormente, y de acuerdo con las normas de protección de datos personales, se sugiere al Consejo Ejecutivo de la Unidad, previa vista del artículo 75 del Decreto 500/091:

Scotiabank Uruguay S.A.: a) se sancione por no cumplir con los principios de la Ley al utilizar datos de personas que no son las que realmente solicitan sus servicios, b) se recomiende se ajusten los tiempos de envíos de los correos electrónicos para no incumplir con los plazos establecidos por la Ley (artículo 14) y verse perjudicado.

El archivo de estos obrados para Tienda Inglesa que actuó conforme a derecho.

Dra. Beatriz Rodríguez

Derechos Ciudadanos

Informe N° 54/019, de 25 de febrero de 2019

Se resuelve una denuncia por publicación en Internet de certificados médicos de una trabajadora luego de culminada su relación laboral**.**

Montevideo, 25 de febrero de 2019

Exp. 2019-008

Denuncia AA con Control Kilos

Informe N° 54

I.- Antecedentes

Con fecha 28 de diciembre de 2018, se presenta ante esta Unidad la Sra. AA a formular denuncia contra el Sr. Daniel Kliman (dueño de la empresa Control Kilos). En su denuncia expresa que se desempeñaba como Nutricionista para el Sr. Kliman en el Centro de Educación para la Salud Control Kilos. Su relación se basaba en un contrato de arrendamiento de servicios profesionales pero que expresa que en los hechos se trataba de un régimen de subordinación, recibiendo órdenes de diverso tipo por parte del Sr. Kliman.

Expresa que la relación se tornó intolerable y eventualmente se consideró indirectamente despedida llevando el trámite a la vía judicial. Indica que cuando el denunciado tomó conocimiento de esta situación la amenazó, le envío mensajes a su celular, y le indicó que *"ya están subidas tus referencias personales, googlea licenciada AA o licenciada en nutrición AA".* Cuando ingresó al sitio web descubrió que se habían publicado los certificados médicos donde se la podía identificar y donde surgía la enfermedad que había padecido. Ante tal situación la denunciante mediante telegrama colacionado lo intimó a que diera de bajas las citadas publicaciones.

Posteriormente, recibió un telegrama del denunciante en el que se le expresaba que podía publicar esa información en base a la libertad de expresión. Después, tuvieron una audiencia de conciliación en la vía judicial, la que fue infructuosa y en la que se solicitó la baja de esos certificados. Con fecha posterior se cambió el contenido de la página web, dándose de baja los certificados médicos y sustituyendo la información por un aviso general de que la denunciante no se desempeña más en la empresa. Se expresa que en la vía judicial se presentó copia simple de los mensajes de whatsapp y acta de comprobación. Adjunta copia simple de impresiones de pantalla (fs. 2 a 28).

De la denuncia se procedió a dar traslado al denunciado, quien tomó vista el 1° de febrero de 2019, y la evacuó el 15 de febrero. En sus descargos expresan que es cierto que la empresa publica en su sitio web que la denunciante no se desempeña más para ellos y aclaran que no se publica ningún otro dato más relativo a la denunciante. Refieren a que la comunicación de datos personales está permitida por el artículo 17 literal b) de la Ley N° 18.331, de 11 de agosto de 2008, que establece que no es necesario el previo consentimiento para la comunicación de datos en los supuestos previstos en el artículo 9° de la misma norma referida en el literal c) a los listados cuyos datos se limitan en el caso de personas físicas a nombres y apellidos, documentos de identidad, nacionalidad, domicilio y fecha de nacimiento. Agregan que *"En el mes de julio del año 2018 y tan sólo durante algunos días fueron publicados certificados médicos en base a los cuales la denunciante lleva adelante una campaña de desprestigio y difamación contra la empresa y la persona del Sr. Daniel Kliman"* (subrayado de la informante).

Indican que dicha campaña tendría por objetivo presentar al Sr. Kliman como responsable de una enfermedad frente a clientes, colegas y público en general desarrollando este argumento. Agrega que existen conductas contrarias por parte de la denunciante, que se debe tener en cuenta que ella era la figura que representaba a la empresa. En definitiva, considera que era una persona de confianza de la empresa y conocida públicamente. Adjunta mensajes de whatsapp, partes de la demanda laboral, copia de contrato laboral, captura de pantalla, copia de poder.

Con fecha posterior, el expediente volvió para informe jurídico.

II.- Análisis

El presente caso versa sobre una posible comunicación de datos personales sin consentimiento del titular, entre ellos datos de salud contenidos en certificados médicos, por parte de la denunciada.

a. Cuestión previa

Cabe puntualizar que en el presente informe no se analizará ninguna cuestión que haga relación con la demanda laboral en virtud de que se trata de un tema que se encuentra fuera de la competencia de esta Unidad. A esos efectos, se tramita ya en la vía judicial el proceso laboral correspondiente siendo las resultancias de este caso totalmente autónomas respecto a lo que se resuelva en la vía judicial.

b. Comunicación de datos personales

Corresponde analizar si la denunciada procedió a publicar sin consentimiento de la titular datos personales, incluyendo datos de salud. Según el escrito de la denunciante surge la publicidad en el sitio web de certificados médicos de fecha 2 de abril de 2018, 30 de abril de 2018, 7 de mayo de 2018, 30 de mayo de 2018 y 7 de mayo de 2018. En ellos, se distingue además de la cédula de la denunciante y el tipo de enfermedad diagnosticada en cada ocasión.

A los efectos de analizar jurídicamente la situación cabe precisar que la denunciada realizó dos tipos distintos de publicaciones. El primero en el cual publicó los certificados médicos de la denunciante con el detalle ut supra y la segunda donde se informa sobre las personas que se encuentran desvinculadas de la empresa indicando solamente sus nombres.

En este marco, corresponde indicar que en términos generales para comunicar datos personales se requiere el previo consentimiento del titular y la existencia de interés legítimo del emisor y del destinatario (art. 17 de la Ley N° 18.331, de 11 de agosto de 2008). Es así que en el segundo caso, donde se listan las personas que no forman parte más de la institución, se estaría cumpliendo con la ley en tanto existe un interés de la institución en informar que determinadas personas no se encuentran más vinculadas a ésta, y no se requeriría su consentimiento por ser aplicable la excepción detallada anteriormente.

En el segundo caso por el contrario, donde se comunican los datos de salud de la denunciante, no surge probado la existencia de ninguno de estos elementos. Tampoco son de aplicación al caso concreto ninguna de las excepciones allí dispuestas. En este sentido, no se comparte la posición del denunciado de ser aplicable el literal c) del art. 9° por remisión del art. 17 por no estar en presencia de un listado sino de un conjunto de certificados médicos referentes a una única persona.

En estos certificados médicos surgen datos de salud, como el tipo de enfermedad padecida así como el lapso de inhabilitación. Por tanto, resulta de plena aplicación lo dispuesto en el artículo 18 de la Ley N° 18.331, de 11 de agosto de 2008, por el cual *"Ninguna persona puede ser obligada a proporcionar datos sensibles. Éstos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito de sus titulares"* (subrayado de la informante). Cabe indicar que el artículo 4° literal e) define a los datos sensibles como *"datos personales que revelen el origen racial y étnico, preferencias políticas, convicciones religiosas o morales afiliación sindical e informaciones referentes a la saluda o a la vida sexual"*.

La publicación de datos sensibles es reconocida por la parte demandada en su escrito, la cual la acota en el tiempo, no siendo éste un elemento suficiente para no considerar lesionados los datos personales de la denunciante. Está nítidamente comprobado que la denunciante de ninguna forma consintió la publicación de esta información, a tal grado que llegó a solicitar en la audiencia de conciliación que se eliminara esa información, cuestión que fue realizada por la denunciada posteriormente. Por tanto, en este aspecto esta informante considera que hay una infracción a la normativa de protección de datos personales.

A ello cabe agregar que la denunciada alega que la denunciante quiere lesionar la reputación de la empresa pero qué cabe decir respecto a la empresa que publica los datos de salud de la denunciada. Es claro que publicar datos sensibles como ser los datos de salud puede causar una afectación a su trabajo como profesional

por lo que no se considera tampoco este argumento de recibo.

En definitiva, debe considerarse que la recolección y el tratamiento de datos sensibles como el que sucede en el caso concreto, el que se realiza sin el consentimiento expreso y escrito del titular, es un caso grave de infracción a la normativa de protección de datos personales.

c. Antecedente

La empresa Control Kilos tiene una denuncia ante esta Unidad por Expediente 2016-2-10-000271 por comunicación de datos sin consentimiento siendo intimida por el Consejo a la inscripción de sus bases de datos, habiendo iniciado el trámite por 3 bases de datos, las cuales sólo una de ella fue culminada y registrada.

III.- Conclusiones

De conformidad con lo analizado en el presente informa, se considera que la denunciada ha realizado un tratamiento de datos personales, incluido sensibles, en infracción a lo dispuesto en el artículo 18 de la Ley N° 18.331, de 11 de agosto de 2008, por lo que se sugiere la imposición de la sanción que el Consejo Ejecutivo entienda corresponder.

Previo a elevar al Consejo, se solicita dar vista previa a la denunciada a los efectos de lo dispuesto en el artículo 75 del Decreto 500/991.

Es todo cuanto tengo que informar.

Dra. Flavia Baladán

Informe Nº 69/019, de 12 de marzo de 2019

Se informa una consulta formulada por el Banco de Previsión Social sobre contestación de oficios judiciales con especial atención a la información referida a montos de prestaciones de actividad y pasividades de afiliados así como otra información de naturaleza sensible.

Montevideo, 12 de marzo de 2019

Exp. 2018/2/10/0000653

Informe N° 69

I.- Antecedentes: Vienen los presentes obrados en atención a la solicitud realizada por el BANCO DE PREVISIÓN SOCIAL referente a la provisión de información al Poder Judicial. Puntualmente hace referencia a la contestación de oficios judiciales y a la información confidencial requerida por los jueces –hace expresa exclusión de la información secreta que se encuentra regulada por el artículo 47 del Código Tributario-.

II.- El tratamiento de los Datos Personales referido por la consultante

En primer lugar cabe destacar que se comparten las referencias normativas y el desarrollo realizado por la consultante en el marco de la situación fáctica planteada.

Se plantea en especial la situación de la comunicación de los montos de las prestaciones de actividad y pasividad de los afiliados, atendiendo a su naturaleza de materia gravada a los efectos de distintas especies tributarias, y por ende – aunque no lo mencionan en la consulta-, potencialmente comprendidas en el secreto tributario.

En este sentido, la opinión del suscrito es que el artículo 47 del Código Tributario tiene un amplio alcance, a decir de ADRIASOLA "(…) en el caso uruguayo el amplio giro de la norma contenida en el artículo 47 del Código Tributario permite afirmar que estamos ante un sistema amplio, por lo cual ingresan dentro de la información amparada por el secreto no solo los datos identificatorios de los contribuyentes, sino también cualquier información vinculada, tales como el monto de los impuestos, contenido de las declaraciones juradas, todo aquello que permita reconstruir el patrimonio o ingresos del contribuyente, etc." (ADRIASOLA, Gabriel. "El delito tributario, la cooperación penal internacional y la extradición". La Justicia Uruguaya, Tomo 126. Sección Doctrina. pág. 85) Y por ende, la entrega de la información señalada – prestaciones de actividad y pasividad- no sólo se encuentra alcanzada por la confidencialidad derivada de su carácter de dato personal, sino por el secreto impuesto por la Ley.

En consecuencia, las hipótesis que motivan su entrega, además del expreso consentimiento para relevarlo que debe dar el propio interesado, se encuentran en el propio artículo 47. Es decir, que la Administración Tributaria deberá, ante cada solicitud realizada por el Poder Judicial, determinar si se encuentra en el marco de las excepciones que prevé la norma o no.

Con respecto a la información sensible, no amparada por normas específicas de derecho tributario, debemos considerar los artículos 17° y 18° de la Ley N° 18.331, de 11 de agosto de 2008.

En este sentido, el consentimiento expreso y escrito no es la única hipótesis que autoriza la revelación de la información de ese carácter. 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 lo que respecta a la comunicación de datos sensibles, el artículo 17° establece las condiciones para que ésta proceda, requiriéndose el interés de emisor y destinatario, y el consentimiento del titular, o encontrarse enmarcado en alguna de las excepciones, siendo de interés mencionar el literal B, que remite a su vez al artículo 9°, cuyo también literal B incluye entre las excepciones los datos que "se recaben para el ejercicio de

funciones propias de los poderes del Estado o en virtud de una obligación legal”.

En nuestra legislación el Poder Judicial es uno de los Poderes del Estado (artículos 233 y siguientes de la Constitución Nacional). La Ley N° 15.750, de 24 de junio de 1985 por su parte establece que “El Poder Judicial y el Tribunal de lo Contencioso Administrativo son independientes de toda otra autoridad en el ejercicio de sus funciones” (Art. 1°).

La provisión de una tutela jurisdiccional efectiva requiere en ocasiones la solicitud y provisión de informaciones que puedan resultar de naturaleza sensible. Máxime cuando el elenco de datos sensibles es relativamente amplio, conforme lo establecido en el artículo 4° de la Ley N° 18.331, de 11 de agosto de 2008 (datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual).

No existiendo otras normas que impongan una protección especial o una calidad particular a la información sensible solicitada, corresponde aplicar en consecuencia los artículos referidos. En ese sentido, acreditado que sea el interés por parte del Juzgado correspondiente, en el marco del artículo 17 literal B y 9 literal B de la Ley N° 18.331, a través de una comunicación por oficio, indicando además expresamente la información solicitada y su fin, para la aplicación a un proceso determinado, corresponderá su entrega.

III.-Conclusión

En conclusión, a criterio del suscrito corresponde informar que:

La información asociada al pago de los tributos recaudados por la consultante se encuentra abarcada por las disposiciones en materia de secreto tributario y por ende sólo podrá ser entregada –aún al Poder Judicial- en los casos expresamente previstos en la norma (no limitado al consentimiento del interesado).

Otra información, aún de naturaleza sensible, podrá ser entregada a requerimiento del Poder Judicial, aún sin contar con consentimiento expreso y por escrito del interesado, siempre que se acrediten las condiciones establecidas en el artículo 17 literal B y en el artículo 9 literal B de la Ley N° 18.331, de 11 de agosto de 2008.

ESC. DR. GONZALO SOSA

Informe N° 69/019 bis, de 12 de marzo de 2019

Consulta remitida por la Dirección Nacional de Aduanas con respecto al alcance del artículo 43 de la Ley N° 19.438, de 14 de octubre de 2016, por el que se faculta a esta Dirección a publicar, entre otra, información de nombres de los importadores y exportadores, además de fechas, número de inscripción en el registro aduanero, valor de aduana, país de origen de destino.

Montevideo, 12 de marzo de 2019

Informe N° 69

Se requiere opinión de esta Unidad con respecto al alcance de lo establecido en el artículo 43 de la Ley N° 19.438, por el que se faculta a la Dirección Nacional de Aduanas a publicar, entre otra, información de nombres de importadores y exportadores, además de fechas, número de inscripción en el registro aduanero, valor de aduana, país de origen y de destino.

Desde la perspectiva de la protección de datos personales, toda revelación de información personal a una persona distinta del titular se configura en una comunicación de datos, regulada expresamente por el artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008.

En este sentido, y fuera del consentimiento informado y previo del titular del dato, las hipótesis en las que la comunicación de datos puede realizarse en legal forma se encuentran reguladas en este artículo y en el artículo 9°, por remisión del primero. Pero además, debe en todos los casos existir un interés legítimo del destinatario y del beneficiario de la pretendida comunicación.

Así, la comunicación de datos personales procede en las situaciones previstas, y además en caso de que:

A) así lo disponga una ley de interés general.

B) en los supuestos del artículo 9° de la presente ley.

C) 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.

D) se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

En ese sentido, esta Unidad ya se ha pronunciado en dictamen N° 27/013, de 8 de agosto de 2013 – referido en el informe que se encuentra agregado en obrados-, N° 1/015 y N° 3/015, ambos del 4 de marzo de 2015. En el punto vinculado a la comunicación de datos de despachantes de aduanas a entidades públicas, se dictaminó en el último de éstos que la DNA se encuentra facultada para recolectar y comunicar datos a otros organismos públicos en el cumplimiento de sus funciones, sin requerir para ello del consentimiento de los involucrados, atento a lo establecido en los artículos 9 literal B y 17 literales A y B de la Ley N° 18.331. Con respecto a restantes comunicaciones de datos, ella corresponde según el dictamina 1 del dictamen N° 27/013, sólo con el previo consentimiento o luego de la aplicación de mecanismos de disociación, o en su defecto, habilitando la publicación de los datos expresamente mencionados en el literal C del artículo 9° en formato de listado. Esto es reiterado además en el dictamen N° 3/015.

Ahora bien, los dictámenes mencionados se fundaban en normativa previa a la sanción de la Ley N° 19.438, de 14 de octubre de 2016, por la que se otorga a la DNA la facultad de realizar la publicación arriba referida, incluyendo determinada información que puede caracterizarse como “personal”. Asimismo, indica que no rige al respecto lo establecido en el artículo 7 del Código Aduanero (aprobado por

el artículo único de la Ley N° 19.276, de 19 de setiembre de 2014), que prevé el secreto de las actuaciones.

Por ende, se concluye que existe una autorización legal para la publicación de la información –siendo de aplicación de lo dispuesto en el artículo 9° literal B por remisión del artículo 17 literal B de la ley citada-. Ahora bien, toda publicación de datos personales –sobre todo si es realizada en internet-, aún autorizada por Ley, debe además basarse en determinados principios que morigeren los impactos eventuales en los derechos de los titulares de esos datos.

De hecho, con respecto a la comunicación al público en general, esta Unidad ya se ha pronunciado en el sentido de minimizar todo riesgo de afectación a las personas por ejemplo en los dictámenes Nº 12/012 de 7 de junio de 2012, 2/014 de 13 de febrero de 2014 y en las Resoluciones Nº 1040/012 de 20 de diciembre de 2012 y 6/016 de 9 de marzo de 2012, entre otras, fundado en el hecho de que nos encontramos ante un derecho fundamental (artículo 72 de la Constitución). Así, en estos dictámenes se proponen distintos mecanismos como la desindexación, y otras técnicas que limitan los impactos en los derechos de las personas.

Debe tenerse presente además, refrendando lo antedicho, que la eximición del secreto de las actuaciones previsto por el artículo referido con respecto a la información publicada, no implica *per se* una excepción a la confidencialidad de algunos de los datos contenidos en ella, por tratarse de información personal.

En conclusión, corresponde sugerir a la DNA realizar un ejercicio de ponderación de derechos previo a la publicación de la información, empleando para ello los criterios ya recomendados por los dictámenes arriba mencionados. Se estima pertinente además ofrecer el asesoramiento de esta Unidad previo a proceder a la mencionada publicación.

Es cuanto tengo que informar.

Dr. Gonzalo Sosa

Informe N° 105/019, de 2 de abril de 2019

Se resuelve una denuncia referida al recibo de mensajes por whatsapp de una empresa del rubro gastronómico.

Montevideo, 02 de abril de 2019

Exp. 2018-2-10-0000454

Ref. DENUNCIA SR. AA CONTRA D´ LA RIBERA

EMPANADAS POR MENSAJE DE TEXTO NO DESEADO

Informe Nº 105

I. Antecedentes

I. La presente viene a consideración de la Unidad Reguladora y de Control de Datos Personales (URCDP), en virtud de la denuncia formulada por el señor AA contra D´la Ribera Prado, por presunto incumplimiento de la Ley N° 18.331 de 11 de agosto de 2008.

II. Expresa el Sr. AA que recibió en su teléfono personal (celular) un WhatsApp de la empresa de empanadas horneadas que se encuentra en la zona del Prado, un mensaje privado, con una promoción de la noche. Indica que le solicitó a la empresa le informe de dónde obtuvo su número telefónica. Agrega que la empresa respondió que “alguna vez habré comprado ahí”.

III. Continúa el denunciante indicando que “jamás me consultaron si deseaba recibir promociones y ofertas a mi teléfono personal, solo lo toman y lo hacen”. Aporta captura de pantalla de los mensajes intercambiados con la empresa (fs. 5 y siguientes).

IV. Según consta a fojas 15 del expediente se dio vista a D´la Ribera Prado, quien se presentó escrito a fojas 21 y siguientes.

V. A fojas 57 se dio vista a Aravo SA (Pedidos Ya), la que presenta escrito a fojas 65 y siguientes.

II. Análisis

I. Surge del escrito presentado por la denunciada que el sistema que utiliza el local de pedidos es el software DELYSOFT, el cual “realiza una carga automática de datos de los datos del cliente cuando se recibe una llamada telefónica, lo cual se logra a través del captor telefónico instalado con el software. Además los recepciona automáticamente vía web o vía sms.”

II. Indica que también utiliza aplicaciones como Pedidos Ya que intermedian entre el cliente y el comercio, “que carga en nuestra base de datos, automáticamente los datos de quien pide comida, ya sea nombre, dirección y correo electrónico.”

III. Agrega que la base de datos se va conformando desde el año 2012, con contactos de clientes, que tanto por teléfono fijo como por celular y/o por Pedidos Ya, han hecho alguna vez un pedido.

IV. En el caso indican que el denunciante “aparece en nuestra base de datos como cliente que alguna vez hizo –al menos- un pedido, desde su celular, para la dirección (…) Si lo hizo a nuestro teléfono fijo, siempre se pide (a través de la conversación telefónica) las calles laterales (…) Si lo hizo por Pedidos Ya, las calles laterales las debe ingresar él, conjuntamente con los demás datos que le exige la aplicación (…) Pedidos Ya envía el pedido remotamente al software DELYSOFT y nuestra impresora imprime un talón”.

V. A fojas 65 de estos obrados Aravo SA (pedidos Ya) indica que “el Sr. AA realizó un único pedido a la empresa D´La Ribera Empanadas (Prado) con fecha 29 de enero de 2018, con número 42368886”, adjunta comprobante.

VI. Pedidos Ya confirma que el procedimiento descripto por la denunciada es correcto, en lo relativo a las compras y operativa. Detalla además se trata de uno de los tres posibles mecanismos que existen para realizar compras a través de la plataforma. En el caso se trata de una integración, es decir, el restaurante "ya cuenta con un sistema operativo para gestionar los pedidos de su restaurante y éste se "integra" con el software de PEDIDOSYA para recibir allí mismo los pedidos realizados a través de la plataforma."

VII. Agrega Pedidos Ya que a través de los mecanismos descriptos "los datos que llegan a los restaurantes son únicamente nombre, dirección y teléfono, que son los datos imprescindibles para que el pedido se pueda entregar y por ende, que el servicio de intermediación de PEDIDOSYA pueda cumplirse correctamente".

VIII. Indica Pedidos Ya que el restaurante asume (según la cláusula cuarta del contrato) la obligación "utilizar la información suministrada por PEDIDOSYA (…) a los únicos efectos de cumplir con su obligación frente al usuario, obligándose a no utilizar, reproducir, almacenar, enajenar, transferir, contactar directamente al usuario, compartir ni de ninguna otra forma disponer, de forma total o parcial de dicha información". Anexa modelo de contrato (fs. 69).

IX. Cabe precisar que de la captura de pantalla agregada por D´ La Ribera Empanadas (Prado) a fojas 25 del expediente, surge que además de los datos detallados por Pedidos Ya en el punto VII, se comunica el correo electrónico del Sr. AA.

X. De los elementos aportados por D´La Ribera Empanadas (Prado) y PEDIDOSYA surge que se comunicaron datos del Sr. Dos Santos para el estricto cumplimiento del pedido gastronómico efectuado, conforme a los términos y condiciones y política de privacidad de esta última. No obstante lo anterior, el envío de promociones efectuado al denunciante por parte D´ La Ribera Empanadas se realiza incumpliendo lo establecido en la cláusula cuatro del contrato (fs. 69).

XI. Por tanto se considera que D´La Ribera Empanadas, ha incumplido lo establecido en el artículo 9° de la Ley N° 18.331, de 11 de agosto de 2008 (LPDP), así como también el artículo 7° de la mencionada ley, relativo al principio de finalidad.

XII. Sin embargo, y de acuerdo a lo detallado por ambas empresas, debe tenerse presente que la integración entre el software DELYSOFT y la plataforma de PEDIDOSYA, no permite diferenciar con claridad qué pedidos ingresan directamente al restaurante y cuáles a través de la plataforma, por tanto, este extremo debe ser corregido a la brevedad para evitar en un futuro situaciones como la que se considera en estos autos.

XIII. Asimismo D´La Ribiera debe tener especial consideración de lo dispuesto en el artículo 21 de la Ley citada, en el sentido de que una vez recibida una solicitud de no envío de promociones, se instrumenten las soluciones técnicas que así lo efectivicen, esto tratándose de clientes propios del local y no respecto de los derivados desde PEDIDOSYA, sobre los cuales no puede ni debe tratar sus datos según el contrato que vincula a ambas empresas.

XIV. Del análisis de los Términos y Condiciones y de la Política de Privacidad de PEDIDOSYA, que luce a fojas 81 y siguientes del expediente no surge con claridad qué datos serán comunicados a los locales gastronómicos, quien es el responsable de la base de datos y ante quién se pueden ejercer los derechos consagrados en los artículos 14 y 15 de la Ley, cuál es la ubicación física de esta, si se realizan transferencias, etc., incumpliéndose así el deber de informar consagrado en el artículo 13 de la LPDP.

XV. Por último, corresponde señalar que no surge registro de base de datos a nombre de la empresa D´La Ribiera (Prado) o Nora Loureiro, existiendo por tanto además contravención de lo establecido en el artículo 6° de la Ley citada.

III. Conclusiones

I. En virtud del análisis efectuado, corresponde señalar que la empresa D´ La Ribera (Nora Loureiro) ha incumplido con las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008, en particular los artículos 6°, 7°, 9° y 21, en cuanto no ha inscripto sus bases de datos, no ha cumplido con el deber de informar al momento de colectar los datos, y lo más relevante ha utilizado éstos sin el consentimiento de su titular. Por lo anterior, se sugiere la aplicación de las sanciones que el Consejo Ejecutivo de la URCDP estime convenientes.

II. Asimismo, la empresa D´La Ribera (Nora Loureiro) deberá informar a sus clientes que sus datos serán incorporados en la base de datos (art. 13 de la Ley), los que podrán ser utilizados para el envío de promociones respetando lo dispuesto en el artículo 21 de la Ley citada.

III. Además se sugiere intimar a la empresa D´ La Ribera (Nora Loureiro) la inscripción de las bases de datos que correspondan en un plazo de 30 días corridos bajo apercibimiento de ulteriores sanciones.

IV. Por otra parte, respecto a la empresa Aravo SA (PEDIDOSYA) se recomienda que: A) al implementar integraciones entre el software propio del restaurante y la plataforma de Pedidos Ya se distinga claramente el cliente propio de aquel que accede a la plataforma cuyos datos se comunican a los efectos de poder cumplir con el pedido. B) modifique su Política de Privacidad, ajustándola a las disposiciones de la Ley N° 18.331, dando cuenta a la Unidad

V. Antes de la aplicación de la sanción, se sugiere previa vista conforme al artículo 76 del Decreto 500/91.

Dra. María Cecilia Montaña Charle

Derechos Ciudadanos

Informe N° 106/019, de 2 de abril de 2019

Se informa una consulta realizada por la Facultad de Veterinaria sobre la posibilidad de grabar los exámenes teóricos tomados en modalidad oral.

Expediente 2019-2-10-0000070

Montevideo, 2 de abril de 2019

Informe N° 106

I. Antecedentes

Vienen los presentes atento a la consulta formulada por la Facultad de Veterinaria respecto a la posibilidad de grabar los exámenes teóricos que se toman en modalidad oral.

La consulta señala que se fundamenta en el planteo realizado por estudiantes y docentes ante el Departamento de Educación Veterinaria, y que fuera elevado a la Comisión de Enseñanza.

Obra en autos un completo informe realizado por la Dra. Nora Sobrino de la Dirección General Jurídica de la Universidad, de fecha 2 de agosto de 2018, en el que se asimila la situación planteada con la video-vigilancia, en función de la definición amplia consagrada en el Dictamen 10/010 de 16 de abril de 2010 del Consejo Ejecutivo de la Unidad.

Si bien se irá a concluir que a criterio del suscrito, sí corresponde la grabación de los exámenes orales, lo es por fundamentos diferentes al esgrimido por la Dirección General Jurídica de la Universidad.

II. Análisis

El Dictamen N° 10/010 refiere a la regulación de la video-vigilancia en el territorio nacional, definida como toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo (Considerando I). Dicha video-vigilancia se encuentra además definida por la finalidad

El hecho de que en el dictamen precitado no se explicite la obligación de obtener el consentimiento, se fundamenta en la circunstancia de que éste -máxime en el caso de la video-vigilancia-, no es sino una de las varias bases legítimas de tratamiento de los datos. Así, el Resultando VIII apartado a, refiere entre las obligaciones de los responsables, el dar cumplimiento a la normativa que los regula, sobre todo en lo referido a la protección de datos personales. Dentro de esta obligación, se encuentra la establecida en el artículo 9° de la Ley N° 18.331, de 11 de agosto de 2008, de recabar el consentimiento previo a la recolección de los datos, o asegurarse de encontrarse abarcado por las excepciones previstas en la norma (que en los hechos funcionan como bases legítimas para el tratamiento de los datos).

A modo de ejemplo, la video-vigilancia en materia de seguridad pública se encuentra excluida de la Ley conforme lo dispuesto en el artículo 3° literal B, y las cámaras instaladas en domicilios particulares se enmarcan dentro de lo dispuesto en el literal A del mismo artículo, por lo que, siempre que se circunscriban a esas actividades y no otras, no se requerirá el consentimiento de los titulares de los datos para la captación de las imágenes. Ello por supuesto, sin perjuicio de la aplicabilidad de los principios en la materia, como ha señalado en reiteradas oportunidades el Consejo Ejecutivo de la Unidad.

En consecuencia, no se trata de una cuestión vinculada a la inexistencia de consentimiento o a un “consentimiento tácito” –imposible de argumentar en nuestro derecho conforme lo establece el artículo 9° de la Ley-, sino al hecho de que determinados tratamientos se encuentran excluidos de la aplicación de las normas, con la excepción indicada en el párrafo anterior.

En el caso planteado por la Facultad de Veterinaria, no existe en principio un tratamiento como el indicado en los párrafos anteriores, por lo que habrá de verse si es necesario el consentimiento de todos los involucrados –docentes, estudiantes y público en general- para proceder a la captación de las imágenes y grabación de sus

voces.

Las instancias de examen y su desarrollo dependen de la reglamentación aprobada para cada Facultad por el Consejo Directivo Central. En el caso de la Facultad de Veterinaria, el CDC aprobó el correspondiente Reglamento el 27 de diciembre de 1967, estableciendo que “Los exámenes se realizarán en acto Público. El resultado se hará saber de inmediato al examinando.” (artículo 15°). El artículo 17° indica que “Contra el resultado del examen no habrá reclamación alguna”. Conforme lo señalado por la Dra. Sobrino, correspondería la modificación de este último artículo atento a los principios de derecho y derechos fundamentales vigentes.

Podría indicarse que la finalidad de la grabación de los exámenes sería proveer de garantías a estudiantes y docentes, a la vez que dotarlos de instrumentos para promover una eventual revisión. A criterio del suscrito, esta situación permitiría equiparar las pruebas orales a las escritas –en las que queda la prueba documental del contenido del examen y las correcciones realizadas-, lo que se visualiza como deseable. Todo ello además, en el marco de los principios de derecho y derechos fundamentales señalados por la Dra. Sobrino.

La Ley N° 12.549, publicada el 29/10/1958 establece que “La Universidad de la República es una persona jurídica pública, que funcionará como Ente Autónomo, de acuerdo con las disposiciones pertinentes de la Constitución, esta Ley Orgánica y demás leyes, y los reglamentos que la misma dicte (Art. 1°).”

Dentro de las atribuciones del Consejo Directivo Central se encuentra la de “h) Dictar los reglamentos necesarios para el cumplimiento de sus funciones, los que se denominaran ordenanzas y especialmente el estatuto de todos los funcionarios de la Universidad, de conformidad con los artículos 58 y 61 de la Constitución” (Art. 21).

En la Ordenanza de Estudios de Grado y Otros Programas de Formación Terciaria (Res. Nº 3 de C.D.C. de 2/VIII/2011 – Dist. Nº 451/11, Res. Nº 4 de C.D.C. de 30/VIII/2011– Dist. Nº 575/11 y 576/11, publicada en el Diario Oficial el 19 de setiembre de 2011) se indica en particular que: “Artículo 37.- La evaluación de los aprendizajes cumplirá una función formativa a la vez que de verificación y certificación. Se emplearán modalidades e instrumentos diversos de aplicación docente, así como mecanismos de auto y heteroevaluación. La misma cumplirá principios básicos de validez, confiabilidad y consistencia con los procesos de enseñanza y de aprendizaje, contribuyendo a la mejora continua de los mismos. Como parte del rol formativo de la evaluación de aprendizajes se deberán establecer instancias de muestras de pruebas, exámenes y demás evaluaciones. (18 en 19)”. Ello refrenda la importancia de contar con mecanismos que permitan una mejor valoración de los exámenes brindados por los estudiantes, no ya por eventuales reclamaciones, sino como parte del propio proceso de aprendizaje.

Dicho esto, la sugerencia de la grabación de exámenes debería estar sujeta a un protocolo que minimice los riesgos de vulnerar los derechos de los titulares de los datos –entre ellos su voz e imagen-. Ello por ejemplo, otorgando a los estudiantes el derecho a que se grabe su voz pero no se filme su imagen, a oponerse a la grabación en su totalidad –asumiendo las consecuencias derivadas de ello-, restringir la grabación de forma que no se capten otras personas que puedan encontrarse en la sala presenciando el examen, permitir el acceso a la información únicamente por parte de las personas involucradas en ese examen específico –profesores que tomaron el examen, autoridades de la enseñanza por cuestiones puntuales y el estudiante involucrado-, y la eliminación de las grabaciones una vez que hayan cumplido la finalidad prevista –muestra de la prueba antes del período siguiente o vencimiento del plazo previsto para plantear acciones contra los resultados de ésta-, además de contar con los mecanismos de seguridad pertinentes en el almacenamiento de la información. A los efectos se sugiere proporcionar a la UDELAR el asesoramiento pertinente, si esta lo estima conveniente.

En conclusión, el suscrito estima que es posible la grabación de los exámenes orales y su almacenamiento, debiendo cumplirse en todos los casos con los extremos referidos en el párrafo anterior.

Es cuanto tengo para informar.

Dr. Gonzalo Sosa

Informe Nº 110/019, de 8 de abril de 2019

Se resuelve una denuncia presentada en relación con la instalación de una cámara de video vigilancia en posible infracción a los requerimientos de protección de datos personales.

Montevideo, 8 de abril de 2019

Exp. 2018-558

Denuncia AA C/ Mercadito Rivera

Informe N° 110

I.- Antecedentes

Mediante informe N° 14, de 21 de enero de 2019, se indicó que se comprobó la existencia de una cámara que apuntaba hacia a entrada del domicilio de la denunciante, la cual carecía de los logos identificatorios y de la cual no existía información el Registro de Base de Datos Personales.

Se presumía que la cámara no fue instalada de conformidad con lo que establece la normativa de protección de datos personales, incluyendo la inexistencia de conformidad de la copropiedad del Edificio con respecto a su instalación. Cuando se procedió a dar vista al Mercadito Rivera, éste no procedió a evacuarla, y en base a todo ello, se procedió a recomendar la imposición de sanciones, previa nueva vista al denunciado (Mercadito Rivera).

Dicho informe se elevó de conformidad al Consejo Ejecutivo de esta Unidad, y éste de mandato verbal dio vista de conformidad con el artículo 76 del Decreto 500/991. Se procedió a notificar al Mercadito Rivera que tomó vista el 22 de marzo del presente año y la evacuó con fecha 6 de abril.

En sus descargos expresa que la empresa ha procedido a retirar la cámara de filmación indicaba que estaba enfocaba alas viviendas en donde se domicilia la denunciante. Adjunta fotos como medios probatorios. Expresan que la cámara fue instalada a efectos de tomar medidas de seguridad y que la empresa que se los instaló no les informó de los requisitos legales existentes.

Con los descargos presentados, el informe pasó para informe jurídico.

II.- Análisis

a. Aplicación de las conclusiones del primer informe.

En términos generales, cabe indicar que las precisiones realizadas con respecto a las medidas que se deben adoptar en materia de videovigilancia continúan siendo aplicables al presente caso.

b. Aplicación de las medidas necesarias para el caso de contar con sistemas de videovigilancia.

Esta informante entiende que la denunciada (Mercadito Rivera) deberá adoptar todas las medidas necesarias para la utilización de sistemas de videovigilancia. Se toma en cuenta que la denunciada informa que no se utiliza más la cámara pero para el caso de que se utilice en otro local, deberá adoptar las medidas oportunamente informadas.

Además, si se realiza videovigilancia donde se graba lo captado, se deberá proceder a inscribir las correspondientes bases de datos.

Cabe acotar que la instalación de la cámara hubiere sido viable jurídicamente si **ésta** se hubiera ajustado a los parámetros legales establecidos por esta Unidad.

c. Conducta punible.

Ahora bien, ello no obsta a indicar que la cámara estuvo instalada por un largo período de tiempo, que es reconocido por la denunciada, que ésta apuntaba a la entrada del edificio de la denunciante, y que dicha cámara no contaba con logos ni con autorización para su instalación. A ello se agrega que no se conoce el

destino de las grabaciones realizadas. No siendo suficiente la expresión de disculpas vertidas en el escrito de descargos.

En virtud de todos estos extremos, esta informante entiende que corresponde la imposición de sanciones a consideración del Consejo Ejecutivo de esta Unidad.

d. Conducta no ajustada a derecho.

Por último, cabe agregar que la conducta de la denunciada es tachable desde el punto de vista jurídico en la medida que cuando se le notificó de la denuncia tomó conocimiento de la situación pero no contestó la vista conferida.

Que solamente cuando se lo intima bajo apercibimiento, y conoce el informe donde se recomienda sanciones, contesta la vista. Es por ello que la conducta de la denunciada no se ajusta ni a la buena fe ni a la lealtad procesal.

e. Deber de informar

De los descargos surge que la cámara fue instalada por una tercera empresa la cual no informó de estos requisitos, por lo que se solicita se informen los datos identificatorios de esta empresa para que tome conocimiento de los procesos y se ajuste a éstos.

III.- Conclusiones

De los descargos presentados, surge probada la existencia de la instalación de una cámara en infracción a la normativa de protección de datos. Que dicha cámara ya no se encuentra operativa pero que con ella se lesionó la privacidad de la denunciante por un determinado período de tiempo, por lo que se recomienda la imposición de la sanción que el Consejo Ejecutivo entienda corresponde al caso concreto.

Asimismo, se recomienda que la denunciada ajuste sus procesos relacionados con videovigilancia a la normativa vigente.

Por último, se requiere a la denunciada (Mercadito Rivera) informe los datos de contacto de la empresa que instaló las cámaras para que ésta tome conocimiento de los actos acaecidos y ajuste sus procesos en materia de videovigilancia.

Es todo cuanto tengo que informar.

Dra. Flavia Baladán

Informe Nº 111/019, de 8 de abril de 2019

Se informa una consulta presentada por el Banco de Previsión Social respecto a la firma de un Acuerdo de Programa con la organización SMILE TRAIN.

Expediente 2019-2-10-0000079

Montevideo, 8 de abril de 2019

Informe N° 111

I. Antecedentes

Vienen los presentes atento a la consulta formulada por el Banco de Previsión Social respecto a la firma de un Acuerdo de Programa con la organización con sede en los Estados Unidos denominada Smile Train.

II. Análisis

Se adjunta por la consultante una propuesta de Acuerdo con la organización sin fines de lucro referida, la que se dedica a la provisión de fondos, herramientas y educación en materia de labio/paladar hendido.

El objetivo del Acuerdo es "*concertar un esfuerzo de cooperación y unión (el "Programa") en el que Smile Train proporcionará financiamiento al proveedor para que el proveedor pueda ofrecer cirugías reconstructivas totalmente gratis y otros servicios relacionados para los pacientes de escasos recursos con labio y paladar hendido que de otra manera no podrían pagar dichos tratamientos*" (cláusula de antecedentes literal C).

La ubicación geográfica de la organización es en Nueva York, Estados Unidos de América y no se encuentra certificada por el acuerdo Privacy Shield, por lo que no se encuentra dentro de la lista de organizaciones "adecuadas" para la realización de transferencias internacionales de datos en el marco de dicho acuerdo, conforme la Resolución del Consejo Ejecutivo de la Unidad N° 4/019, de 12 de marzo de 2019.

Con respecto al BANCO DE PREVISIÓN SOCIAL, éste ostenta un rol preponderante en el tratamiento de los casos referidos en la consulta, atento a lo dispuesto por el Decreto-Ley N° 15.084, de 28 de noviembre de 1980, el decreto N° 227/981, de 27 de mayo de 1981 y demás normas reglamentarias. El alcance de dicho rol, y el trabajo realizado a través del CRENADECER (Centro de Referencia Nacional de Defectos Congénitos y Enfermedades Raras) puede consultarse en el documento del proyecto, expedido por la Dirección Técnica de Prestaciones, la Gerencia de Prestaciones de Salud y la Gerencia de Asistencia Médica de dicho organismo.

En lo que refiere al acuerdo en sí, corresponde señalar en primer lugar, con respecto a la protección de datos en general, que la participación en el Programa depende a su vez de la participación en Smile Train Express, que según el punto 4 de las obligaciones del proveedor (en este caso el BANCO DE PREVISIÓN SOCIAL) se trata de una base de datos de cuidado del labio/paladar hendido gratuita y global, con información de registro del paciente completa –incluyendo el formulario de consentimiento-. Afirma la cláusula que el formulario de registro del consentimiento estará sujeta a las leyes aplicables con relación a la liberación de la información médica.

A fs. 22 de estos obrados se encuentra el expediente médico del paciente que tendrá su cirugía apoyada por Smile Train. Dicho formulario indica cual es la naturaleza de la entidad, que mantiene expedientes médicos con información de salud relevantes, y fotos de los pacientes tomadas antes y después de la cirugía. Por otra parte, se informa que el uso de esos expedientes es con propósitos de revisiones de calidad quirúrgica, educación, evaluación y relaciones públicas, sin perjuicio de las actualizaciones en los tipos de datos, que menciona se darán a conocer.

Asimismo, se informa que los datos estarán disponibles para personas autorizadas en la base de datos a la que puede accederse a través de la web, informando Smile Train que no compartirá la información con terceras partes no autorizadas. Asimismo, se procura asegurar la implementación de estándares de seguridad –aunque no los detalla- y su acceso por parte de los titulares de los datos. Resulta de interés señalar que Smile Train

eliminará el nombre e información de salud de la base de datos a solicitud del titular del dato.

Posteriormente se hacen unas breves referencias al funcionamiento de la Base de datos (folio 30), indicando el mecanismo para el envío de los usuarios y las contraseñas.

Se trata en el caso de una transferencia internacional de datos en el marco de una comunicación de datos, que en buena parte son datos sensibles –de salud-, resultando por ende aplicables los artículos 17°, 18° y 23° de la Ley N° 18.331, de 11 de agosto de 2008. También deben considerarse la aplicación de los principios previstos en los artículos 8° a 12° de la Ley, con una especial referencia a la nueva redacción del artículo 12° dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018.

El artículo 17° de la Ley indica que toda comunicación de datos personales –entendida ésta como una revelación de información personal a un tercero distinto del titular- debe efectuarse con el consentimiento informado de éste (o en el marco de alguna de las excepciones previstas en el mismo artículo, o las del artículo 9° por remisión expresa), y además debe realizarse en interés del emisor y del destinatario del dato. En el caso de que la comunicación se sustente en el consentimiento, éste siempre será revocable.

El artículo 18 de la Ley por su parte indica que todo tratamiento de datos sensibles debe realizarse con el consentimiento expreso y escrito del titular, cuando medien razones de interés general autorizadas por ley, cuando el organismo tenga mandato legal para hacerlo o con fines estadísticos o científicos –en este último caso disociado de sus titulares-.

En este caso, se prevé expresamente que los padres brinden el consentimiento para la comunicación de la información a SMILE TRAIN a través del modelo de consentimiento que se adjunta al presente expediente. Dicho modelo de consentimiento deberá revisarse en su redacción –o complementarse en debida forma-, principalmente en lo que respecta a la posibilidad de establecerse finalidades adicionales a las informadas, ya que no resulta claro cómo se efectuará esa comunicación y quién es que toma la decisión –aunque presumiblemente sea SMILE TRAIN-.

Pero además, en el caso se prevé una comunicación a un destino no adecuado, que está expresamente prohibido por el artículo 23° de la Ley mencionada, con las siguientes excepciones:

"1) Cooperación judicial internacional, de acuerdo al respectivo instrumento internacional, ya sea Tratado o Convención, atendidas las circunstancias del caso.

2) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado por razones de salud o higiene públicas.

3) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable.

4) Acuerdos en el marco de tratados internacionales en los cuales la República Oriental del Uruguay sea parte.

5) Cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

También será posible realizar la transferencia internacional de datos en los siguientes supuestos:

A) Que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista.

B) Que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado.

C) Que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero.

D) Que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

E) Que la transferencia sea necesaria para la salvaguardia del interés vital del interesado.

F) Que la transferencia tenga lugar desde un registro que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para su consulta."

En el presente caso, existiendo un consentimiento brindado por el interesado, en forma previa, informada y escrita, ya sea para sí o para su representado –en legal forma-, la situación de hecho podría encontrarse abarcada por lo dispuesto en el literal A del artículo mencionado.
En lo que respecta al consentimiento en el tratamiento de los datos de salud, a efectos de garantizar un consentimiento libre, expreso, escrito, informado e inequívoco –como el exigido para la transferencia internacional de datos de salud de un exportador a un importador que reviste la naturaleza de tercero-, este no puede encontrarse relacionado con la necesidad de que se le provea un tratamiento específico, cuando éste debe proveerse a las personas al amparo de obligaciones legales impuestas a organismos encargados de la salud pública. Recordemos que la Constitución en el artículo 44° establece que "*El Estado legislará en todas las cuestiones relacionadas con la salud e higiene públicas, procurando el perfeccionamiento físico, moral y social de todos los habitantes del país.*
Todos los habitantes tienen el deber de cuidar su salud, así como el de asistirse en caso de enfermedad. El Estado proporcionará gratuitamente los medios de prevención y de asistencia tan sólo a los indigentes o carentes de recursos suficientes".
Sin perjuicio de lo indicado, existe profusa legislación vinculada a las obligaciones y deberes del Ministerio de Salud Pública, la Administración de Servicios de Salud del Estado, el Banco de Previsión Social, entre otros, alguna de las cuales se mencionaron en el presente informe.
Por su parte, tanto el artículo 72 de la Constitución como el artículo 1° de la Ley N° 18.331, reconocen otros derechos inherentes a la personalidad humana –específicamente el derecho a la protección de datos personales- que debe ser objeto de las garantías apropiadas.
En definitiva, este informante no observa inconvenientes en que se solicite a los padres de los menores que serán sujetos a procedimientos financiados por SMILE TRAIN –y sólo respecto de éstos- consentimiento para la remisión de la información clínica concerniente a dicho procedimiento. Debe resultar claro además que en caso de negativa el menor tendrá la posibilidad de obtener la asistencia debida en el marco de las obligaciones inherentes a las entidades en el marco del Sistema Nacional Integrado de Salud, y de las disposiciones específicas en materia de este tipo de enfermedades.
También deberá limitarse la entrega de la información a la estrictamente necesaria para el cumplimiento de las obligaciones asumidas con SMILE TRAIN y no otra, y asegurarse la supresión de ésta a requerimiento del interesado por una vía sencilla y gratuita. Esta manifestación, al igual que el consentimiento para el envío de la información, podrá ser realizada por el menor una vez adquirida la capacidad legal o por su representante. En caso de que no resulte claramente la forma de ejercer los derechos, el BANCO DE PREVISIÓN SOCIAL deberá asumir la obligación de recabar esas manifestaciones de voluntad y de que se dé cumplimiento a lo solicitado por los titulares de los datos o sus representantes.
Toda otra hipótesis de comunicación de información que no se sustente en el consentimiento en las condiciones mencionadas deberá realizarse previo proceso de disociación de datos, procurando en todos los casos garantizar la anonimización de dicha información.
En lo que respecta a las restantes obligaciones en el marco del artículo 12° de la Ley N° 18.331, en la redacción dada por el artículo 39 de la Ley N° 19.670, este caso requiere claramente de la adopción de medidas especiales a efectos de garantizar el cumplimiento de los principios en materia de protección de datos, sugiriéndose a la consultante la realización de una Evaluación de Impacto en la Protección de Datos.
Por otra parte, también deberá registrarse la base de datos de los menores que formen parte del programa, declarando a la entidad estadounidense SMILE TRAIN como encargada de tratamiento, teniendo presente

además que: a) Esta transferencia de información deberá ser informada y considerada por su delegado de protección de datos (el que deberá ser designado obligatoriamente en atención a lo dispuesto por el artículo 40 de la Ley N° 19.670); y b) Deberá comunicarse a SMILE TRAIN que por el tipo de información que gestiona se encontrará alcanzada por las disposiciones de la ley N° 18.331.

Es cuanto tengo para informar.

Dr. Gonzalo Sosa

Informe N° 113/019, de 9 de abril de 2019

Se resuelve una denuncia referida al cumplimiento del derecho de supresión.

Montevideo, 9 de abril de 2019.

Expediente N° 2019-2-10-0000081.

Denuncia Sr. AA contra ADT Uruguay

por ejercicio de derecho de supresión

Informe jurídico Nº 113

I. Antecedentes

Con fecha 15 de marzo de 2019 presenta ante la Unidad Reguladora y de Control de Datos Personales (URCDP), el Sr. AA una denuncia contra ADT Uruguay (ADT Security Services S.A.), por no cumplimiento del ejercicio de supresión.

El denunciante solicita se inicien las actuaciones correspondientes por la Unidad. Así se procede a dar vista de estos obrados a través de telegrama colacionado al denunciado, presentándose a tomar la vista respectiva y sus aclaraciones.

II. Argumentos

El denunciante manifiesta que la denunciada lo ha estado llamando varias veces sin su consentimiento debido a que él no es cliente y nunca lo ha sido. Presentó formulario de supresión ante la empresa denunciada y esta no quiso firmar ni sellar el formulario como acuse de recibo (fojas 1 y 2).

Se dio vista a la denunciada, la que manifiesta que de acuerdo con el artículo 15 de la Ley N° 18.331 informa que los datos de denunciante fueron suprimidos de su base de datos (foja 29).

III. Análisis

Del análisis de las aclaraciones presentadas por ambas partes se desprende que: el denunciante ha recibido llamadas a su teléfono de parte del denunciado sin su consentimiento, incumpliendo así el art. 9° de la Ley N° 18.331.

De igual forma sucede con el derecho de supresión ejercido por el denunciante ante la empresa denunciada que no ha querido firmar ni sellar el formulario presentado ante ella. Consecuentemente no ha cumplido con el plazo de 5 días que establece el art.15 para realizar la supresión de los datos del denunciante de su base de datos, realizándolo recién casi un mes después que se hubiera generado el hecho, como lo confirma en el escrito presentado a foja 29.

En suma, se entiende que la denunciada ha incumplido con el principio de previo consentimiento informado (art.9°) y con el derecho de supresión de los datos del denunciante de su base de datos.

Por lo tanto, en relación con lo informado anteriormente, se sugiere al Consejo Ejecutivo de la Unidad, previa vista del artículo 75 del Decreto 500/091, la aplicación de la sanción correspondiente de acuerdo con la Resolución N° 105/015, de 13 de diciembre de 2015.

Dra. Beatriz Rodríguez

Derechos Ciudadanos

Informe Nº 184/019, de 27 de junio de 2019

Se informa una consulta realizada por el Instituto de Regulación de Cannabis (IRCCA) sobre el tratamiento correcto a conferir a los datos históricos, teniendo en cuenta que la justicia penal podría solicitar datos sobre personas así como la pertinencia de solicitar autorización para la conservación de datos con fines históricos, estadísticos o científicos.

Montevideo, 27 de junio de 2019

Exp. 2019- 240

Consulta IRCCA sobre Ley de protección de datos personales

Informe N° 184

I.- La consulta

Se presenta ante esta Unidad una consulta por parte del Instituto de Regulación y Control de Cannabis (en adelante IRCCA).

Esta Entidad Pública indica que es responsable de una base de datos, la que se encuentra registrada ante la URCDP. Expresan que los datos concretos que se asientan en dicha base de datos respecto de los adquirientes de cannabis, como adquiriente en los locales de expendio, cultivadores domésticos y miembros de los Clubes Cannábicos de Membresía, son considerados datos sensibles de acuerdo con lo dispuesto en el artículo 3° del Decreto Ley N° 14.294, en la redacción dada por el artículo 5° de la Ley N° 19.172, de 20 de diciembre de 2013.

Expresan que en relación con el tratamiento de datos personales, requieren la opinión de la Unidad respecto a dos temas puntuales:

- Se indique cuál es el tratamiento correcto para conferirle a los datos históricos. Teniendo presente que la Justicia Penal puede llegar a solicitar datos sobre personas, cuyos registros no se encuentran vigentes.
- Si debe el IRCCA, a tales efectos, solicitar de acuerdo con lo dispuesto en el artículo 37 del Decreto N° 414/009, autorización de conservación de datos para fines históricos, estadísticos o científicos.

II – Análisis

a. **Cuestiones preliminares**

Conforme con la Ley N° 19.172, de 20 de diciembre de 2013, se pretende promover y mejorar la salud pública de la población mediante una política orientada a minimizar los riesgos y a reducir los daños del uso del cannabis.

En este marco, la citada norma establece que el Estados asumirá el control y la regulación de las actividades de importación, exportación, plantación, cultivo, cosecha, producción, adquisición a cualquier título, almacenamiento, comercialización y distribución del cannabis y sus derivados.

A esos efectos se crea el Instituto de Regulación y Control del Cannabis (IRCCA) como persona pública no estatal encargado de llevar todos los temas vinculados al uso de cannabis.

Conforme con el artículo 8 de la citada norma se crea el registro: *"…llevará sendos registros para las excepciones previstas en los literales A), B), C), D), E), F) y G) del artículo 3° del Decreto-Ley N° 14.294, de 31 de octubre de 1974, en la redacción dada por el artículo 5° de la presente ley.*

Las características de dichos registros serán objeto de reglamentación por parte del Poder Ejecutivo.

La información relativa a la identidad de los titulares de los actos de registro tendrá carácter de dato sensible para lo establecido en los literales E) y F) del artículo 5° de la presente ley, de conformidad con lo dispuesto por el artículo 18 de la Ley N° 18.331, de 11 de agosto de 2008.

El registro del cultivo, según la legislación vigente, será requisito indispensable para poder ampararse en

las disposiciones de la presente ley. Cumplidos ciento ochenta días desde la puesta en funcionamiento del referido registro, el que no tendrá costo para los usuarios y se hará para asegurar la trazabilidad y control de los cultivos, solo se admitirán registros de plantíos a efectuarse".

Esta norma fue posteriormente reglamentada por cuatro decretos, a saber:

- Decreto Nº 128/016 de 02 de mayo de 2016,
- Decreto Nº 46/015 de 04 de febrero de 2015,
- Decreto Nº 372/014 de 16 de diciembre de 2014,
- Decreto Nº 120/014 de 06 de mayo de 2014.

Es de destacar que el decreto N° 120/014, regula con carácter general los artículos de la Ley N° 19.172, entre sus artículos 52 a 77 regula el *"Registro del Cannabis".*

b. **Sobre la primera consulta**

El IRCA consulta sobre el tratamiento que se le debe conferir a los datos históricos, o sea, sobre aquellos datos que recaen un vencimiento de los plazos de registro, una baja voluntaria o una sanción.

Cabe comenzar por indicar que resulta de plena aplicación las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008, ya que se trata de la posibilidad de conservar datos personales (de conformidad con lo dispuesto en su artículo 4°, literal d que brinda la definición de dato personal). Asimismo, se debe indicar que algunos de los datos personales son declarados sensibles de acuerdo con el artículo 8° de la citada Ley N° 19.172.

Que respecto al tiempo de conservación de los datos personales, se debe considerar el artículo 8° de la mencionada Ley N° 18.331 que establece con carácter general que "*Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados*.

La reglamentación determinará los casos y procedimientos en los que, por excepción, y atendidos a los valores históricos, estadísticos y científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya perimido tal necesidad o pertinencia" (subrayado de la informante).

Esta informante entiende que respecto al tiempo de conservación hay que actuar de acuerdo con este criterio general ya que las normas que regulan todo lo que tiene que ver con el cannabis, no establecen en ningún lugar un plazo específico de conservación de los datos, transcurrida la finalidad para la cual fueron recabados.

Sin perjuicio de ello, si debe tenerse en cuenta que el Decreto N° 120/014, cuando regula el "*Registro de Cannabis"* establece en las distintas secciones del Registro criterios para la conservación de los datos personales.

Es así que según el artículo 52 de este Decreto quienes desarrollen algunas de estas actividades deberán inscribirse en la sección correspondiente del Registro.

Conforme con el artículo 53 de esta norma, el IRCCA es el organismo encargado del Registro de Cannabis. Específicamente, y a vía de ejemplo, según el artículo 57 las licencias para la plantación, producción y distribución de Cannabis psicoactivo para dispensación en farmacias, mantendrán su vigencia por el período y en las condiciones que se establezca al otorgarse la misma. Por su parte, las licencias para el cultivo doméstico de Cannabis psicoactivo, para clubes de Membresía y sus miembros, tendrán una vigencia de tres años, pudiendo reinscribirse a su vencimiento.

Por otro lado, el artículo 58, indica que la licencia a Farmacias para la dispensación de Cannabis psicoactivo tendrá vigencia por el mismo período establecido por el Certificado de habilitación expedido por el Ministerio de Salud Pública.

Es importante remarcar que según el artículo 59, las personas registradas en las Secciones de Cultivo Doméstico, Clubes de Membresía o Adquirentes de Cannabis, podrán solicitar ser dados de baja de la

sección registral respectiva, en cualquier momento.

Y así, en adelante, hay plazos de conservación de los datos establecidos hasta el artículo 77 de dicha norma.

Cabe indicar asimismo, que ha sido criterio de esta Unidad, indicar que cuando existan razones legales suficiente, como por ejemplo acciones civiles o penales, se podrán conservar los datos pero en forma bloqueada. Esto es, no permitiendo su tratamiento de datos. Cabe indicar que según el Decreto N° 414/009, el bloqueo de datos es un *"procedimiento mediante el cual se reservan datos con el fin de impedir su tratamiento, excepto para ser puestos a disposición de los Poderes del Estado, o instituciones que estén legalmente habilitadas, a los efectos de atender las posibles responsabilidades surgidas del tratamiento"* (artículo 4° literal a).

Ahora bien, extinguida la finalidad original por la cual se conservan los datos personales, y transcurrido el plazo de posibles acciones legales civiles o penales, corresponde la eliminación de toda la información por principio general, salvo que se acrediten razones históricas, estadísticas o científicas basadas en la legislación específica que permitan su conservación.

Por último, cabe indicar que sobre la consulta realizada sobre la entrega de información solicitada por la Justicia Penal, es de plena aplicación el Dictamen N° 16/2018, de 11 de setiembre de 2018, de esta Unidad. Es necesario solamente indicar que se deberá proceder a la entrega de la información cuando ésta efectivamente exista, indicándose en caso contrario que no existe la información solicitada por la causal que corresponda al caso concreto (vencimiento del plazo, sanción, etc.).

c. **Sobre la segunda consulta.**

Específicamente, el IRCCA consulta si se debe solicitar autorización para conservar los datos personales por razones históricas, científicas o estadísticas.

En este sentido, se indica que el artículo 8° de la Ley N° 18.331, de 11 de agosto de 2008 permite este procedimiento. Además, se debe considerar que el artículo 37 del Decreto N° 414/009, de 31 de agosto de 2009, regula el procedimiento de conservación para fines históricos, estadísticos o científicos.

Esta última norma establece que el procedimiento para la autorización de conservación de datos personales con estos fines se iniciará siempre a petición del responsable que pretenda obtener la declaración.

Además, indica que en el escrito de solicitud, el responsable deberá identificar el tratamiento de datos al que pretende aplicarse la excepción, establecer las causas que justificarían la declaración, presentar las medidas que el responsable de la base de datos se propone implantar para garantizar el derecho de los ciudadanos, y acompañar los documentos necesarios para justificar su solicitud. También la norma indica que previo a adoptar resolución, la URCDP puede solicitar la opinión de instituciones, organismos, públicos o privados, que tengan competencia o mérito para ser consultados en relación al caso.

Por tanto, si la institución quiere conservar datos personales en este marco, deberá proceder de acuerdo con el procedimiento que a esos efectos describe el artículo 37 del citado Decreto 414/009.

III.- Conclusiones

En relación con la primer consulta realizada por el IRCCA, vinculada con el tiempo de conservación de los datos personales, se debe aplicar el artículo 8° de la Ley N° 18.331, de 11 de agosto de 2008, el cual indica que se pueden conservar en tanto exista las razones por las cuales se recolectaron. A ese respecto, la normativa específica del sector prevé plazos especiales para la conservación de los datos personales en los distintos sectores que conforman el Registro de Cannabis

Asimismo, se pueden conservar los datos aun cuando se venzan los plazos establecidos si existe un fundamento legal para su conservación (por ejemplo acciones civiles o penales) pero siempre bloqueados, no pudiendo mantenerse más allá de ese plazo.

Vencidos todos los plazos descritos ut supra, se debe proceder a la eliminación de los datos pudiendo

conservarlos solamente por razones históricas, científicas o estadísticas, siguiendo el procedimiento que el Decreto N° 414/009, establece a esos efectos.

Es todo cuanto tengo que informar.

Dra. Flavia Baladán

Informe N°218/019, de 12 de agosto de 2019

Se resuelve una denuncia referida a la presunta falta de respuesta ante el ejercicio del derecho de acceso.

Montevideo, 12 de agosto de 2019

Exp. 2019-000140

Denuncia AA con DNIC

Informe. N° 218

I.- Antecedentes

Se presenta ante esta Unidad el Sr. AA quien expresa que el 12 de marzo de 2019 habría realizado ante la Dirección Nacional de Identificación Civil (en adelante DNIC), Departamento de Gestión Documental, una solicitud de acceso a la información personal que sobre su persona existiera en la citada Entidad. Indica que hasta la fecha (21 de marzo de 2019) no ha recibido respuesta a su solicitud y en DNIC solamente le han expresado que espere a que lo llamen (fs. 2 a 7).

Con fecha 30 de abril del presente año, se solicitó dar vista de la denuncia a la DNIC, el telegrama fue debidamente entregado, y la DNIC tomó vista con fecha 3 de mayo de 2019 (fs. 8 a 14).

Transcurrido el plazo de 10 días hábiles sin evacuar la vista, el expediente volvió a la informante quien solicitó dar vista nuevamente a la Entidad para que la evacuara.

Que con fecha 2 de julio de 2019, se realizó el informe jurídico N° 140, en el, cual se indicó que se está en presencia de un ejercicio de derecho de acceso por parte del denunciante, que se presume que surge que transcurrió el plazo legalmente establecido sin haber contestado por lo que la conducta puede ser pasible de sanción y se solicitó dar vista previa de acuerdo con lo dispuesto en el Decreto N° 500/991 (fs. 24 y 25).

El 25 de julio del corriente año el expediente pasó para agregar documentación proveniente del Ministerio del Interior. Ésta consiste en un expediente tramitado ante dicha Entidad Pública de la cual, surge que el 26 de marzo del corriente al se realiza un análisis jurídico de la solicitud, el 2 de mayo un análisis técnico, y que el 9 de mayo comparece el denunciante a tomar vista de las citadas actuaciones. El 8 de julio se vuelve a realizar un dictamen jurídico, cuya copia es entregada al Sr. Pereira con fecha 12 de julio del corriente año. Con fecha 16 de julio de 2019 se procedió a remitir las actuaciones a esta Unidad.

El 25 de julio de 2019, el expediente volvió nuevamente para informe jurídico.

II.- Análisis

En primer lugar, corresponde indicar que respecto a las consideraciones generales sobre el derecho de acceso esta informante se remite a lo considerado en el informe N° 140, de 2 de julio de 2019, que luce en el presente expediente.

Que respecto a las actuaciones remitidas por el Ministerio del Interior cabe indicar que se procedió a efectivizar el ejercicio del derecho de acceso del titular de los datos, entregando a éste la información solicitada.

Sin perjuicio de ello, se debe considerar que la solicitud fue presentada en marzo de este año y el dictamen fue notificado el 8 de julio, excediendo ampliamente los plazos previstos en el artículo 14 de la Ley N° 18.331, de 11 de agosto de 2008. Se debe tener en cuenta que además se procedió a dar una vista previa al denunciante con fecha 9 de mayo, fecha que también excede ampliamente los plazos establecidos.

Asimismo, es importante tener en consideración que la Dirección Nacional de Identificación Civil se encuentra regulada por una normativa específica, sobre todo lo que hace relación con la composición del número de identificación que luce en los documentos de identidad.

Es importante tener presente que según el artículo 34 de la Ley N° 18.331, de 11 de agosto de 2008, la URCDP tiene como cometido controlar la observancia del régimen legal (literal d). Conforme con el art. 35 de la citada

norma, el órgano de control puede aplicar sanciones a los responsables de bases de datos o encargados, en caso de que violen las normas de la presente ley, las que se graduarán en atención a la gravedad reiteración o reincidencia de la infracción cometida.

III.- Conclusiones

De conformidad con lo analizado en el presente informe, la Dirección Nacional de Identificación Civil accedió al ejercicio del derecho de acceso pero fuera de los plazos establecidos por el artículo 14 de la Ley N° 18.331, de 11 de agosto de 2008, por lo que está informante sugiere al Consejo la imposición de la sanción que estime corresponde al caso concreto.

Asimismo, se sugiere que la DNIC adecué sus procesos a los efectos de cumplir con los plazos legalmente establecidos en estos casos.

Es todo cuanto tengo que informar.

Dra. Flavia Baladán

Informe Nº 276/019, de 30 de agosto de 2019

Se informa una consulta formulada por el Consejo de Educación Técnico Profesional sobre la posibilidad de contar con una base de datos visible en el sitio web de la institución que contenga identificación de las personas (nombre completo, C.I., título obtenido, nivel que se obtiene con él, plan en que cursó y centro educativo), la situación del trámite del título incluyendo la repartición en que se encuentra y fecha.

Montevideo, 30 de agosto de 2019

Exp. 2019- 340

Consulta de la Prosecretaria del Consejo de Educación Técnico Profesional

Informe N° 276

I- La consulta

Se presenta ante esta Unidad la Prosecretaria del Consejo de Educación Técnico Profesional consultando sobre la posibilidad de contar con una base de datos visible en el sitio web de la institución que contenga: identificación de la persona con nombre completo, cédula de identidad, título obtenido, nivel que se obtiene el mismo, plan en que cursó y centro educativo. Asimismo, el trámite del título con la repartición en que se encuentra y fecha.

Explica que sería un apartado en el sitio web a que se accedería ingresando el nombre de la persona o su cédula de identidad, y se desplegaría una ventana con los datos antes referidos.

En ese marco, se solicita conocer si para instrumentar una base de datos de este tenor, se requiere el previo consentimiento a efectos de proceder a publicar esos datos.

II – Análisis

El caso de marras trata de la legalidad de realizar una comunicación de datos, consistente en la publicación de una base de datos donde surja información de los títulos obtenidos, o su proceso de aprobación, por aquellas personas que cursen educación técnica profesional.

A efectos de su análisis corresponde comenzar por expresar que la comunicación de datos se encuentra definida en el artículo 4° literal b) de la Ley N° 18.331, de 11 de agosto de 2008, el cual indica que es *"toda revelación de datos realizada a una persona distinta del titular de los datos".*

Para realizar comunicación de datos, el artículo 17 de la misma norma, en sede de derechos referentes a la comunicación de datos, indica que los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos. Asimismo, esta norma hace referencia a los casos en los cuáles no es necesario recabar el consentimiento. Sobre este punto, cabe indicar que no resultan de aplicación las excepciones contenidas en los literales a) a d) de la misma norma así como tampoco las excepciones contenidas en el artículo 9° en sede de principio de previo consentimiento informado.

Más específicamente, no aplica ninguna de las excepciones porque no existe una norma de interés general, no son datos de salud y no hay un procedimiento de disociación. Tampoco los datos provienen de fuentes públicas, no provienen del ejercicio de funciones propias de los poderes del estado o en virtud de una obligación legal. No se trata de un listado con datos mínimos, no deriven de una relación contractual, científica o profesional, y tampoco se realiza por personas físicas para su exclusivo personal, individual o doméstico.

En cuanto al consentimiento, éste se encuentra definido en el artículo 4° literal c) como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne*". Por su parte, el artículo 9° de la misma norma regula que el tratamiento regula el consentimiento cuando se haya consentido con esas características. Esta misma norma regula las excepciones

en las cuales no es necesario recabarlo, las cuales tampoco resultan aplicables al caso concreto.

Otro aspecto de análisis es el impacto de la publicación en Internet de este tipo de datos. En este sentido, se debe tener en cuenta el principio de veracidad regulado en el artículo 7° de la Ley N° 18.331, indicando que los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la que se obtuvieron.

Por tanto, desde esta perspectiva, al no ser aplicable ninguna de las excepciones, establecidas, ni normas que mandaten su publicación, se estima que no corresponde en consecuencia su publicación sin el consentimiento de los titulares.

Es importante además hace referencia a un caso similar que se resolvió por Dictamen N° 5/2016, de 9 de marzo de 2016, que indica que la información que emane de la escolaridad universitaria contiene datos personales, que los datos que allí lucen requieren previo consentimiento del titular para ser tratados, que la comunicación de los datos contenidos en la escolaridad universitaria no encuadra en ninguna de las excepciones previstas en los literales a) a d) del artículo 17 de la Ley, así como tampoco en las previstas en el artículo 9° de la Ley N° 18.331, de 11 de agosto de 2008.

Se recuerda además, que conforme con las modificaciones introducidas por la Ley N° 19.670, específicamente el nuevo artículo 39, los responsables y encargados de bases de datos deben adoptar las medidas técnicas y organizativas que correspondan para asegurar su protección (privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, etc.). Por su parte, el artículo 40 de la misma norma establece que todas las Entidades Públicas deben designar un delegado de protección de datos personales, quien deberá asesorar en la formulación, diseño, y aplicación de políticas de protección de datos personales. Además, de dar cumplimiento a los demás principios y derechos de la ley como ser registrar la base de datos, dar cumplimiento al derecho de información, entre otros.

III.- Conclusiones

Que en conclusión, a los efectos de la publicación de la información mencionada en internet es necesario recabar el previo consentimiento informado los titulares de los datos, no siendo aplicable ninguna de las excepciones allí previstas.

Además, deberá tratar los datos de acuerdo con los principios de la normativa de protección de datos personales según lo detallado en el presente informe.

Es todo cuanto tengo que informar.

Dra. Flavia Baladán

Informe Nº 281/019, de 2 de setiembre de 2019

Se informa una consulta remitida por la Secretaría Nacional para la lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAFT) acerca de la posibilidad legal de esa Secretaría de publicar las resoluciones que imponen sanciones a los sujetos obligados.

Montevideo, 2 de setiembre de 2019

Exp. 2019-2-10-0000345

Consulta SENACLAFT sobre publicación en el sitio web

de Resoluciones de sanciones aplicadas

Informe N° 281

I.- La consulta

Se presenta consulta ante esta Unidad por parte de la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAFT).

En la misma se plantea que es intención de la Senaclaft de publicar en la web las resoluciones de sanciones que han sido aplicadas por incumplimiento de la normativa vigente en materia de prevención del Lavado de Activos/Financiamiento del Terrorismo.

De acuerdo a lo anterior, se solicita obtener la opinión de esta Unidad, para lo que se plantean las siguientes consultas:

1) Sobre la posibilidad legal de esa Secretaría para publicar las resoluciones que imponen sanciones a los sujetos obligados y, en caso afirmativo;

2) Qué datos se pueden publicar y cuáles no.

Asimismo, a vía de ejemplo de lo que se publicaría, se adjuntó un modelo de Resolución que impone una sanción de multa a un sujeto obligado para consideración de esta Unidad.

Sin perjuicio de lo anterior, se consulta sobre la posibilidad de publicar en la web de esa Secretaria las resoluciones que imponen sanciones a los sujetos obligados y en tal caso, cuál debería ser el contenido de las mismas a efectos de un correcto cumplimiento de las normas que regulan la protección de datos personales.

II – Análisis

a. **Cuestiones preliminares**

Como bien señala la SENACLAFT en su consulta, en el art. 4 de la Ley 19.574 se establece dentro de los cometidos de la misma, el control del cumplimiento de las normas de prevención de lavado de activos y financiamiento del terrorismo así como ejecutar las sanciones pecuniarias impuestas.

El artículo 4 de la Ley 19.574 de 20 de diciembre de 2017 expresa que *"…La Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo, como órgano desconcentrado dependiente directamente de la Presidencia de la República, diseñará las líneas generales de acción para la lucha contra el lavado de activos y el financiamiento del terrorismo. La misma actuará con autonomía técnica, y tendrá los siguientes cometidos: (…)*

E) El control del cumplimiento de las normas de prevención de lavado de activos y financiamiento del terrorismo por parte de los sujetos obligados por el artículo 13 de la presente ley. (…)

H) Ejecutar las sanciones pecuniarias que imponga mediante resolución…"

Por su parte el artículo 13 establece: "*...El incumplimiento de las obligaciones previstas para los sujetos obligados por el presente artículo determinará la aplicación de sanciones por parte de la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo. Dichas sanciones se aplicarán apreciando la entidad de la infracción y los antecedentes del infractor y consistirán en apercibimiento, observación, multa o suspensión del sujeto obligado cuando corresponda, en forma temporaria, o con previa autorización judicial, en forma definitiva. Las suspensiones temporarias no podrán superar el límite de tres meses. El monto de las multas se graduará entre un mínimo de 1.000 UI (mil unidades indexadas) y un máximo de 20.000.000 UI (veinte millones de unidades indexadas) según las circunstancias del caso, la conducta y el volumen de negocios habituales del infractor…*"

Asimismo se aclara que el procedimiento administrativo tendiente a la aplicación de las referidas sanciones se tramita por el Decreto N° 500/991, culminando –de corresponder- con la aplicación de una sanción de apercibimiento, observación, multa o suspensión o en su caso el archivo, previo conocimiento del interesado.

b. **Sobre la primera consulta**

De acuerdo a lo que surge del modelo de Resolución adjunto, los datos que se proporcionarían del sujeto obligado serían solamente el nombre o razón social y número de identificación (cédula de identidad o RUT, según corresponda).

Según lo dispuesto en el art. 4 literal D) de la Ley N° 18.331 de la Ley de Protección de Datos Personales (en adelante "la LPDP"), los datos identificatorios mencionados tienen el carácter de dato personal.

Asimismo, el literal B) del art. 4 mencionado anteriormente define el concepto de comunicación de datos, y dispone que se trata de: "*toda revelación de datos realizada a una persona distinta del titular de los datos.*"

El art. 17 de la LPDP expresa que: *"Derechos referentes a la comunicación de datos. Los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.*

El previo consentimiento para la comunicación es revocable.

El previo consentimiento no será necesario cuando:

A) así lo disponga una ley de interés general.

B) en los supuestos del artículo 9° de la presente ley.

C) 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. (*)

D) se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate."

En relación con el literal B), los supuestos del artículo 9° de la ley son los siguientes: a) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación, b) se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, c) se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas

jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma, d) deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento, e) se realice por personas físicas para su uso exclusivo personal, individual o doméstico.

Por su parte, el art. 9 – BIS establece que se consideran como públicas o accesibles al público, determinadas fuentes, entre las cuales se encuentran: "*Todo otro registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos puedan ser consultados, difundidos o utilizados por parte de terceros. En caso contrario, se podrá hacer uso del registro o publicación mediante técnicas de disociación u ocultamiento de datos personales*."

Asimismo, el art. 18 de la LPDP establece que: *"Los datos relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas, sin perjuicio de las autorizaciones que la ley otorga u otorgare. Nada de lo establecido en esta ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren inconveniente."*

Por tanto, de acuerdo a lo consultado por la SENACLAFT y a la normativa relacionada, se aplicarían las excepciones al previo consentimiento en este caso y se podrían publicar las Resoluciones.

Debe tenerse presente que el dato personal contenido en las resoluciones no reviste la calidad de público, sino que el mismo es estrictamente personal y su comunicación deberá ceñirse a los principios establecidos en la LPDP.

Además de lo establecido precedentemente, esta informante entiende que la publicación de la Resolución es sin perjuicio de la clasificación o calificación que se realice por parte de dicha Secretaría de la información contenida en el expediente, esto es, información confidencial o reservada, la cual deberá extenderse a todo el expediente así como a su resolución.

Es importante mencionar que la publicación de las resoluciones con los datos personales de los obligados que fueron sancionados implica que la información sobre los mismos quede publicada en un sitio web, y algunas veces sin un tiempo determinado de conservación.

Es por esto que entendemos que nos encontramos ante un caso de ponderación de derechos en conflicto. Dado que por un lado está el deber de transparencia de la SENACLAFT, y por otra parte, el derecho de la persona de preservar su identidad o que dicha información no quede a perpetuidad.

Es importante tener en cuenta que "*La ponderación no es una conciliación, no consiste en encontrar equilibro entre dos principios en conflicto, sino que uno de los dos principios es aplicado prevaleciendo sobre el otro.*

Hay que mencionar que el resultado óptimo de un ejercicio de ponderación no habría de ser el triunfo aplastante de uno de los principios, ni siquiera en el caso concreto, sino la armonización de ambos, la búsqueda de una solución intermedia que en puridad no diera satisfacción plena a ninguno, sino que procurara la más liviana lesión de ambos.

De acuerdo con la doctrina alemana la ponderación es una parte del principio de proporcionalidad, que consta de tres subprincipios: los principios de idoneidad, necesidad y proporcionalidad en sentido estricto. Los tres principios expresan la idea de la optimización. Los derechos fundamentales como principios, son mandatos de optimización". (Subrayado de la informante)

A dichos efectos, se deben tener presentes los criterios de indexación para evitar conflictos con la protección de los datos personales del sujeto obligado. A los efectos de aplicar criterios de indexación para evitar la violación de la protección de los datos personales, nos remitimos a lo establecido en la Resolución N°

1040/2012 de fecha 20 de diciembre de 2012 de la Unidad Reguladora y de Control de Datos Personales.

Sin perjuicio de lo anterior, resulta importante señalar la relevancia que posee el art. 18 de la LPDP que se reseñara anteriormente, en el cual se establece que las autoridades públicas podrán comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren conveniente.

b) cuáles datos deberían publicarse.

En cuanto a la segunda consulta por parte de la SENACLAFT, y en base a lo anterior, esta informante entiende que se deberían mantener los datos que sean necesarios para emitir la Resolución o los cuales surjan como necesarios.

CONCLUSIONES

En base a lo manifestado anteriormente, se concluye que las Resoluciones pueden ser publicadas en el portal de la SENACLAFT sin perjuicio de aplicar ciertos criterios de desindexación de datos.

Es todo cuanto tengo que informar.

Dra. Esc. Lylian Massarino

Informe Nº 289/019, de 6 de setiembre de 2019

Se informa una consulta formulada por la Dirección Nacional de Empleo del Ministerio de Trabajo y Seguridad Social (DINAE) con respecto al Sistema de Intermediación Laboral y la publicación de información de menores de edad.

Exp.- 2019-2-10-0000252

Informe N° 289

Montevideo, 6 de setiembre de 2019

Vienen los presentes obrados atento a la consulta del Ministerio de Trabajo y Seguridad Social con respecto a la necesidad de contar con el consentimiento de los padres de menores de edad que publiquen perfiles laborales en la Plataforma Vía Trabajo.

-ANTECEDENTES DE ESTOS OBRADOS-

En este caso deben buscarse compatibilidades entre las normas que establecen la protección frente al empleo juvenil con la protección de datos personales.

En ese sentido, corresponde tener presente las disposiciones establecidas en los artículos 213 y siguientes del Código Civil (en especial el artículo 267 referente al peculio industrial, entre otros), el Código de la Niñez y la Adolescencia (en particular el Capítulo XII, artículos 161 a 180) y la Ley N° 19.133, de 20 de setiembre de 2013, sobre fomento del empleo juvenil.

En lo que respecta a la protección de datos personales, corresponde considerar las disposiciones de la Ley N° 18.331, de 11 de agosto de 2008, y su decreto reglamentario N° 414/009, de 31 de agosto de 2009.

-ANÁLISIS DEL CASO-

El derecho a la protección de datos personales es un derecho fundamental, inherente a la personalidad humana conforme lo establece el artículo 1° de la Ley N° 18.331. Por otra parte, este derecho se ha convertido en uno de los pilares de los gobiernos digitales responsables, en tanto procura transformarse en un límite a los tratamientos de datos que puedan generar perjuicios a las personas, vulnerando su esfera más íntima, y de esta forma su libertad y su dignidad.

En función de ello, nuestro sistema de protección de datos establece ciertos principios aplicables a toda operación de tratamiento que tiene como centro, la existencia de determinadas bases legítimas que justifican tales operaciones. El consentimiento informado se erige como la principal de esas bases, sin perjuicio de existir otras, todas establecidas en el artículo 9° de la Ley.

Cuando se trata de consentimiento de menores de edad, desde la perspectiva de la protección de datos personales, no existen normas específicas que habiliten un consentimiento – ni siquiera parcial- para el tratamiento de sus datos, como si lo hacen otras normas a nivel internacional (ver por ejemplo el artículo 8 del Reglamento General de Protección de Datos de la Unión Europea relativo a las condiciones para el consentimiento de niños en relación con los servicios de la sociedad de la información). Por ende, la regulación de las normas en materia de protección de datos debe verse cumplimentada a este respecto con las normas en materia civil que regulan la representación de los menores de edad.

En consecuencia de lo antedicho, resultan de aplicación a la obtención del consentimiento para el tratamiento de los datos personales, las disposiciones referidas a la patria potestad y en su caso a la tutela de los menores de edad. Así, se requeriría en función de las disposiciones antes citadas, el consentimiento de los progenitores o tutores para el tratamiento de los datos de sus menores hijos o tutelados.

Por otra parte, las propias disposiciones en materia de habilitación para el desempeño de tareas laborales en el caso de los adolescentes prevén como prerrequisito, el consentimiento de sus responsables –no necesariamente sus padres, pero sí responsables legales-. Véase a este respecto el artículo 167 del Código de la

Niñez y la Adolescencia, que establece la obligación de los adolescentes de contar con carné de habilitación en el que deberá constar, entre otros: “D) Consentimiento para trabajar del adolescente y sus responsables”.

Por ende, con respecto al desarrollo de tareas laborales, el consentimiento del adolescente no resulta suficiente, debiendo complementarse con la de sus responsables. Esto se ve refrendado por lo dispuesto en el artículo 7° de la Ley N° 19.133, que indica que para ser contratado el adolescente requiere, entre otros requisitos “el carné de trabajo habilitante otorgado por el Instituto del Niño y Adolescente del Uruguay”.

Ahora bien, el tratamiento de datos personales refiere a un derecho diferente al antedicho, y por ende contiene regulaciones distintas pero complementarias a éstas. Debemos preguntarnos entonces: ¿la autorización otorgada por los responsables para realizar tareas laborales es suficiente o no para la publicación de la información del menor en una oferta laboral? Desde esa perspectiva, el suscrito estima que, en tanto el consentimiento para el trabajo se encuentra dado en el propio carné de habilitación laboral, y que para el efectivo ejercicio del derecho al trabajo la oferta a través de la publicación es necesaria, esa publicación también se encuentra abarcada por dicho consentimiento. Corresponde sí señalar que esta interpretación se limita exclusivamente a las ofertas realizadas a través del mecanismo informado en estos obrados, en tanto este es controlado por el Ministerio de Trabajo y Seguridad Social, órgano competente para la promoción de la inserción laboral de jóvenes conforme la Ley N° 19.133 y la protección integral de todos los trabajadores.

Por otra parte, también es responsabilidad del Ministerio de Trabajo y Seguridad Social la determinación de la información estrictamente necesaria de los menores habilitados para trabajar en la página señalada y de la adopción de las medidas de seguridad pertinentes, además del cumplimiento de todos los principios y requisitos previstos en la Ley N° 18.331. En ese sentido, se observa como deseable que en la determinación de la información de menores de edad y en los mecanismos para el acceso y tratamiento de esta, se de participación al Instituto del Niño y el Adolescente de Uruguay (INAU), en función de lo dispuesto en los artículos 161 y siguientes del Código de la Niñez y la Adolescencia.

En conclusión, el suscrito estima que es necesario el consentimiento de los representantes de los menores para la publicación de información de menores de edad en el portal vía trabajo, el que puede inferirse del consentimiento dado para el cumplimiento de tareas laborales y que surge del carné de habilitación laboral. Sin perjuicio de ello, es responsabilidad del Ministerio de Trabajo y Seguridad Social arbitrar todas las medidas para el cumplimiento de los principios de la Ley N° 18.331 en la publicación de datos de menores de edad en el portal Vía Trabajo, para lo cual se estima conveniente sugerir la participación del INAU.

DR. GONZALO SOSA

Informe Nº 305/019, de 13 de setiembre de 2019

Se informa una consulta presentada por el Colegio Nueva Cultura sobre la publicación de informaciones vinculadas a denuncias realizadas por madres de alumnos del colegio, a través de páginas web de medios periodísticos nacionales.

Montevideo, 13 de setiembre de 2019

INFORME Número 305

-ANTECEDENTES-

Vienen los presentes obrados atento a la consulta formulada por el COLEGIO NUEVA CULTURA, respecto de la aplicabilidad de la Ley de Protección de Datos Personales y Acción de "Habeas Data" Nº 18.331, de 11 de agosto de 2008, a la situación indicada en la consulta.

En concreto, la consultante señala que ha sido sujeta a la publicación de informaciones respecto a hechos que fueron de conocimiento público y habrían sido dilucidados por la justicia penal competente, pero que continúan apareciendo en distintas publicaciones accesibles a través de los motores de búsqueda.

- LA LEY URUGUAYA Y SUS ÁMBITOS DE APLICACIÓN.

EL ASPECTO SUBJETIVO-

Conforme lo establece la normativa nacional (artículo 1º de la Ley Nº 18.331), "*El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República*". Es decir que nos encontramos frente a un Derecho Humano, merecedor de todo el amparo que brinda las normas nacionales e internacionales de defensa de los derechos humanos en general.

Cabe hacer referencia en el ámbito internacional, al Pacto de San José de Costa Rica de 1969 - base del sistema interamericano de promoción y protección de los derechos humanos-, que en su artículo 11 indica que: "*Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.*

Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

Este derecho, al igual que los restantes explicitados en el Pacto, debe ser objeto de la protección debida por los Estados. Así, el artículo 1º del Pacto establece que: "*1. Los Estados Partes en esta Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna por motivos de raza; color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social*".

A nivel nacional, la Ley Nº 18.331 en su artículo 3º prevé que el régimen "*(…) será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado".* Se describe de esa forma el ámbito objetivo, indicando en concreto que todo tratamiento de dato, sin importar la forma en que éste sea realizado, está abarcado por la Ley.

La Ley no aclara el alcance de su ámbito subjetivo, sin perjuicio de indicar en el Principio de Responsabilidad (artículo 12º) que el responsable de la base de datos es responsable por el cumplimiento de la Ley. Sí se pronuncia el decreto Nº 414/009, de 31 de agosto de 2009, que en su artículo 1º establece: "*El derecho a la protección de los datos personales se aplica a las personas físicas, directa o indirectamente, a través de cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que refiera a ellas.*

Por extensión se aplica a las personas jurídicas, las que gozarán del régimen tuitivo en cuanto corresponda".

Desde el punto estrictamente subjetivo, los sujetos obligados conforme lo indicado por la Ley en el artículo 4º son los siguientes:

"*H) Encargado del tratamiento: persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.*

K) Responsable de la base de datos o del tratamiento: persona física o jurídica, pública o privada, propietaria de la base de

datos o que decida sobre la finalidad, contenido y uso del tratamiento.

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

Si bien la Ley es clara al sostener la responsabilidad de los responsables de tratamiento, no ha adoptado la misma postura con respecto a los encargados. No obstante, el Consejo Ejecutivo de la Unidad ha manifestado que el encargado de tratamiento es pasible de ser sancionado si no da cumplimiento a los preceptos de la Ley. Así ha sido explicitado en el Considerando V de la Resolución Nº 104/2015 de 23 de diciembre de 2015, Considerando III de la Resolución Nº 105/2015 de la misma fecha, todo en el marco del artículo 35º de la Ley Nº 18.331, en la redacción dada por el artículo 152 de la Ley Nº 18.719, de 27 de diciembre de 2010.

En lo que respecta al titular de los datos, la aplicación extensiva de la Ley puede ser discutible en caso de personas jurídicas, sin perjuicio de lo cual parece claro a criterio de este informante, que la afectación en la información disponible a través de la red no impacta únicamente en la Asociación Civil consultante sino además para quienes lo integran y los alumnos y padres que forman parte de dicha institución educativa.

Finalmente, corresponde hacer una referencia al ámbito territorial, consagrado a nivel legal recientemente en el artículo 37 de la Ley N° 19.670, de 15 de octubre de 2018, y que amplía el inicialmente determinado en el decreto 414/009, abarcando actividades de tratamiento realizadas por encargados y responsables ubicados en el exterior del país.

-EL DERECHO AL OLVIDO-

Se ha señalado en otras oportunidades que el Derecho al Olvido consiste en: "*(…) la manifestación de los tradicionales derechos de cancelación y oposición aplicados a los buscadores de internet. El 'derecho al olvido' hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información).*" (Fuente: Agencia Española de Protección de Datos).

El derecho al Olvido como concepto autónomo deriva de la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 13 de mayo de 2014, asunto C-131/12 (coloquialmente conocido como Caso Costeja). En dicha sentencia se analizó la aplicabilidad de la Directiva de la Comisión de la Unión Europea Nº 95/46/CE a tratamientos de datos realizados fuera de la UE que afectan a personas situadas en su territorio, y la aplicabilidad del derecho de cancelación a los motores de búsqueda, a quienes la sentencia considera como responsables de tratamiento.[1]

El Reglamento General de Protección de Datos Personales número 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, refiere al derecho al olvido como una manifestación del derecho de supresión en su artículo 17º. Este derecho posee limitaciones, indicadas en el artículo (ejercicio del derecho a la libertad de expresión e información, cumplimiento de una obligación legal, razones de interés público en el ámbito de la salud públicas, con fines de archivo, investigación científica, histórica o estadística, y para la formulación, ejercicio o defensa de reclamaciones).

Al aclarar los alcances del citado derecho, el Reglamento establece que los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el Reglamento.

Conforme indica PAZOS [2] "*El derecho al olvido, en este caso claramente una concreción del derecho a la cancelación o supresión de datos, desde luego no se corresponde con la facultad reconocida en la sentencia Google Spain y Google. En definitiva, la utilización de la expresión "derecho al olvido" con múltiples y diferentes significados es un fenómeno que persiste e incluso se ha acentuado con el desarrollo del mundo digital. En este contexto, parece aconsejable emplear una denominación diferente y específica para el derecho que consiste en exigir la eliminación de uno de los resultados de la lista ofrecida por el motor de búsqueda, para el caso de que se lleva a cabo una búsqueda a partir de un nombre de una persona, cuando esta persona desea que uno de los resultados no sea mostrado (porque le resulta perjudicial o no), y siempre que no haya un interés público en que ese resultado se mantenga fácilmente accesible a los internautas. Siguiendo el título de este apartado, una posibilidad sería hablar de un "derecho a la oscuridad digital", poniendo el énfasis en los efectos prácticos que conlleva*".

Con respecto al "derecho al olvido" a nivel nacional, se ha hecho referencia a este como una extensión o mutación de los derechos de cancelación, supresión u oposición, en el marco de los principios de finalidad y veracidad consagrados en las normas que regulan la protección de datos personales (artículos 7, 8, 14 y 15 de la Ley Nº 18.331, de 11 de agosto de 2008) [3].

Se ha señalado en concreto por la Unidad que: "*La Unidad Reguladora y de Control de Datos Personales (URCDP) ha tramitado denuncias presentadas contra determinados organismos públicos, que mantienen en la web información del personal, que les causa un perjuicio a su imagen profesional, a su honor y dignidad.*

En estos casos la Unidad resuelve realizar una serie de recomendaciones, sin cuestionar los cometidos legales que se atribuyen por ley a estos organismos, ni el uso de las herramientas tecnológicas a efectos de mejorar la gestión. El problema no

es la legitimidad de la publicación en sí misma, sino el derecho de los titulares a tener el control de sus datos personales, en relación con el tiempo de conservación (la finalidad) y la necesidad real de que dicha información de carácter personal persista para siempre publicada en la web (exista o no un interés público).

A tal fin la URCDP dictó la Resolución N° 1040/2012 de 20 de diciembre de 2012, a través de la cual resuelve recomendar lo indicado 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". [4]

La Resolución Nº 1040/012 de 20 de diciembre de 2012 propuso soluciones técnicas para evitar la indexación de contenidos e inclusión en el caché de los buscadores y recomendó la aplicación de criterios técnicos para la publicación de contenidos en sitios web a fin de controlar la propagación de documentos o sus copias, y minimizar los efectos sobre la protección de datos personales.

A su vez, el Dictamen Nº 2/014 de 13 de febrero de 2014 señala que esel responsable del contenido del sitio web, quien decida la información a ser publicada, y por cuánto tiempo, al igual que los controles o filtros para evitar la indexación por los motores de búsqueda. Ello fue reiterado en la Resolución Nº 6/016 de 9 de marzo de 2016.

El dictamen 17/2016 precitado, explícitamente señala que:*"en la situación planteada por la consultante el titular de los datos incluidos en publicaciones en internet, podrá ejercer el derecho de supresión establecido en el artículo 15 de la Ley Nº 18.331 ante el editor de las páginas web en su calidad de responsable de tratamiento" (Dictamina 1)*.

En oportunidad de informar en el expediente 2016-2-10-0000360, que dio mérito al dictamen 17/2016 de 14 de setiembre de 2016, este informante ha manifestado su opinión de que los motores de búsqueda son, de principio, encargados de tratamiento en todas aquellas situaciones en las que obra como intermediario entre el editor de la página web y el internauta. Se decía que en esos casos, el motor no decide respecto de la finalidad, contenido y uso del tratamiento ni es el propietario de la base.

No obstante, la existencia de múltiples actividades desarrolladas por los buscadores, el hecho de conservar información necesaria para la realización de las búsquedas y la forma de presentar los resultados, entre otros, permiten llevar a reconsiderar la opinión precitada, y sostener que los motores de búsqueda pueden ser considerados responsables de tratamiento. El hecho de que se brinden opciones para la supresión o eliminación de la información coadyuvan a dicha interpretación.

En el caso específico del buscador Google Search, la propia empresa reconoce la existencia de situaciones frente a las cuales sería pertinente la eliminación de la información, máxime cuando esta es de contenido difamatorio. Sin que ello importe un pronunciamiento a favor de las hipótesis previstas por la empresa para la eliminación de la información, estas se encuentran disponibles en la siguiente página web: https://support.google.com/legal/troubleshooter/1114905?rd=1#ts=1349036.

¿Cómo impacta ello en los derechos con los que cuentan los titulares de los datos? ¿Cómo aplicar la ley uruguaya a empresas que se encuentran fuera del territorio nacional?

Actualmente, la aplicación de las normas vinculadas al ámbito territorial depende de la realización por parte de encargado o responsable de tratamiento de actividades vinculadas a la provisión de bienes o servicios a personas situadas en Uruguay o relacionadas con el análisis de su comportamiento. Y en ese sentido los motores de búsqueda se encuentran alcanzados por las disposiciones precedentes. Por ende, en opinión de este informante, es posible plantear ante las empresas proveedoras de motores de búsqueda, cuando se vean afectados derechos de personas en el territorio nacional, un derecho de supresión o rectificación o actualización en los términos y bajo las condiciones previstas en el artículo 15 de la Ley Nº 18.331.

Independientemente de ello, se observa como compleja la posibilidad de contar con mecanismos internos para la eliminación de la información de los buscadores, al no poseer éstos un representante en el país, ni tratar datos con medios situados en éste, aun cuando por la naturaleza de las operaciones de tratamiento que realizan, puedan ser considerados como responsables de tratamiento en el sentido de la Ley Nº 18.331. Por ello, se vislumbra como necesaria la formulación de un nuevo marco normativo que expanda el alcance que debe necesariamente brindar la ley, en aplicación de las normas constitucionales -internas- e internacionales en la materia.

No obstante, considerando la necesidad de contemplar este tipo de situaciones, la existencia de mecanismos internacionales de colaboración se hace fundamental para poder generar actividades conjuntas de investigación y de persecución de violaciones a las normas en materia de protección de datos personales. La participación de nuestro país en el Convenio Nº 108 del Consejo de Europa y su Protocolo Adicional provee el marco necesario para efectivizar estas medidas de colaboración entre las partes, pudiendo aplicarse en el caso concreto, los mecanismos previstos en los artículos 13 y 14 del Convenio, lo que podrá tramitarse a través de esta Unidad.

-LA PONDERACIÓN DE DERECHOS-

En lo que respecta a la información contenida en distintos medios de prensa, aquí corresponde considerar la cuestión del equilibrio entre el derecho a la protección de datos personales y otros derechos como el derecho a la libertad de prensa y la libertad de expresión.

La Protección de Datos Personales es un derecho fundamental, lo que se ve refrendado por el artículo 1º de la Ley Nº 18.331. Pero ello no significa que sea un derecho absoluto. De hecho, Cabe recordar que la Suprema Corte de Justicia ha afirmado en reiteradas sentencias [5] que: "*Tal como lo expresara la Corporación, ni el derecho de usar y disponer de la propiedad ni ningún otro derecho reconocido por la Constitución reviste el carácter de absoluto; un derecho ilimitado sería una concepción antisocial.*

Reglamentar un derecho, es limitarlo, es hacerlo compatible con el derecho de los demás dentro de la comunidad y con los intereses superiores de esta última".

En lo que respecta a la libertad de expresión, PEREZ LUÑO señala la importancia del Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información ya que remite a la Convención Europea de Derechos Humanos, que en particular en sus artículos 8 y 10 regula el derecho al respeto de la vida privada y familiar y el derecho a la libertad de expresión respectivamente. Señala el autor que: "*(…) ambos derechos no son considerados como absolutos e ilimitados, al estar previsto que pueda condicionarse su ejercicio por medidas necesarias, en una sociedad democrática, para garantizar la seguridad, la salud, la moral o los derechos y libertades de los demás (arts.8.2 y 10.2). Este planteamiento normativo ha sido asumido por la Carta de los Derechos Fundamentales de la Unión Europea proclamada en Niza en diciembre de 2000. (…) En ella se reconocen también el derecho a la vida privada (art.7) y a la libertad de expresión y de información (art.11) de los ciudadanos europeos. Se declara, asimismo, en este texto la prohibición de un ejercicio abusivo de los derechos y libertades allí reconocidos (art.54). Pero, tiene especial interés la alusión expresa en la carta a la protección de los datos de carácter personal. En efecto, se establece en su artículo 8 que: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedarán sujeto al control de una autoridad independiente". Esta disposición supone una importante garantía para la tutela de la intimidad de los ciudadanos europeos frente a cualquier tipo de injerencia indebida en esa esfera perpetrada a través de la Red. La libertad de expresión a través de los servicios audiovisuales y, en consecuencia, de Internet no es ilimitada en el seno de la Unión Europea, si bien, sus limitaciones deben ser admitidas restrictivamente. No en vano la libertad de prestar servicios, también en la esfera de la información y la comunicación, es una de las libertades básicas reconocidas en el Tratado de la Unión*" [6].

La Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos, en la Declaración de Principios sobre Libertad de Expresión reconoció un conjunto de principios, y en particular estableció en el quinto el deber de los Estados de prohibir la censura previa, interferencia o presión directa o indirecta sobre cualquier expresión, opinión o información difundida a través de cualquier medio de comunicación. Resulta de interés el décimo principio, por hacer expresa referencia a las leyes de privacidad al sostener que: "*Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles, en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas*".

La mencionada Declaración de Principios pone el centro de la ponderación entre privacidad y libertad de expresión, en el interés público. ¿Y qué es el interés público? Se trata de un concepto jurídico indeterminado respecto del cual debe buscarse una definición. Señala ESCOLA que el interés público es "*(…) el resultado de un conjunto de intereses compartidos y coincidentes de un grupo mayoritario de individuos, que se asigna a toda la comunidad como consecuencia de esa mayoría, y que encuentra su origen en el querer axiológico de esos individuos, apareciendo con un contenido concreto y determinable, actual, eventual o potencial, personal y directo respecto de ellos, que pueden reconocer en él su propio querer y su propia valoración, prevaleciendo sobre los intereses individuales que se le opongan o lo afecten, a los que desplaza o sustituye, sin aniquilarlos.*" [7]

DURAN [8] por su parte realiza un interesante análisis vinculado a la confusión entre interés público e interés general. Señala que en doctrina ALESSI y BANDEIRA DE MELLO distinguen el interés público primario -como el interés de la colectividad como un todo- del interés público secundario -aquel que poseen las entidades públicas como cualquier persona, independientemente de su calidad de servidores de los intereses de la colectividad-. DURAN señala que en nuestro sistema normativo el interés general se asemeja al interés público primario y el interés público, al interés público secundario.

En el aspecto que estamos analizando actualmente, es el concepto de interés público primario o interés general el que debemos manejar, máxime en tanto estamos refiriéndonos a potenciales limitaciones de derechos humanos fundamentales (en el marco de lo establecido en el artículo 72 de la Constitución Nacional).

El "Derecho al Olvido" tal y como se encuentra planteado en la consulta de marras, pone en juego la protección de datos personales, la libertad de prensa y la libertad de expresión, por lo que resulta imprescindible efectuar un adecuado ejercicio de ponderación.

Señala Laura NAHABETIAN en "Protección de Datos Personales vs. Acceso a la Información Pública. ¿Derechos Fundamentales en Conflicto?" que "*Es fundamental encontrar conexiones entre los derechos fundamentales y evitar los conflictos, siendo que como en el caso la colisión es absolutamente excepcional y la opción contraria transformaría la situación*

en conflictos devenidos en situaciones insuperables que sólo podrían salvarse mediante la determinación de una supremacía absoluta de un derecho sobre otro, lo que no es viable a la luz de lo consagrado ya no a nivel legislativo sino constitucional y jurisprudencial" [9].

Afirma además la autora mencionada que pueden existir casos en los que el interés público deba prevalecer sobre el individual, y que a los efectos de una debida ponderación en la resolución de eventuales conflictos deberán de considerarse los criterios de idoneidad, necesidad y proporcionalidad. Todos ellos en el marco general de la aplicación del principio de proporcionalidad desarrollado por Robert Alexy en "La fórmula del peso" [10].

En todos los casos, los responsables y encargados de tratamiento deberán efectuar sus propios ejercicios de ponderación aplicando, en lo pertinente y ante la solicitud de determinados titulares de datos afectados, procurar adoptar soluciones que sean lo menos lesivos a sus derechos, buscando en todos los casos un equilibrio.

No obstante, atento a la naturaleza de los derechos y a la situación planteada, existiendo informaciones de diversa índole vinculadas a la consultante publicadas en la web, si el responsable y encargado omitieran efectuar una ponderación en los términos señalados, ésta corresponderá eventualmente al Poder Judicial, en caso de iniciarse la acción mencionada.

Es cuanto tengo que informar.

ESC. GONZALO SOSA

[1] PIÑAR MAÑAS, José Luis. "APLICACIÓN EXTRATERRITORIAL DE LA DIRECTIVA 95/46/CE SOBRE PROTECCIÓN DE DATOS Y DERECHO AL OLVIDO FRENTE A LOS MOTORES DE BUSQUEDA. COMENTARIO RÁPIDO A LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNION EUROPEA DEL 13 DE MAYO DE 2013, CASO GOOGLE" en "Revista Latinoamericana de Protección de Datos Personales" Año 1 Nº 1. Ed. CDYT. Coordinador: Dr. Pablo Palazzi.

[2] PAZOS CASTRO, Ricardo. "El mal llamado "derecho al olvido" en la era de Internet". Boletín del Ministerio de Justicia. Gobierno de España. Año LXIX. Núm. 2183. Noviembre 2015. Págs. 53 y sigs.

[3] AGESIC. Observatorio Jurídico. Notas de Interés: Derecho al Olvido. Disponible en https://www.agesic.gub.uy/innovaportal/file/3549/1/derecho_al_olvido.pdf. Acc. 22/4/2018.

[4] URCDP. Nota de interés: Derecho al Olvido. Disponible en: https://datospersonales.gub.uy/wps/wcm/connect/urcdp/2ef5f1d1-7f5b-47e7-8972-0241b51fbef6/Derecho+al+olvido.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=2ef5f1d1-7f5b-47e7-8972-0241b51fbef6. Acceso: 28/4/2018.

[5] Ver en particular Sentencias Nº 54/2004, 141/2004, 261/2004 y 697/2014.

[6] PEREZ LUÑO, Antonio Enrique. "INTERNET Y LOS DERECHOS HUMANOS". Anuario de Derechos Humanos. Nueva Época. Vol. 12. 2011. Págs. 287-330

[7] Ver referencia realizada por DE CORES, Carlos y CAL, Juan Manuel en "EL CONCEPTO DE INTERÉS PÚBLICO Y SU INCIDENCIA EN LA CONTRATACIÓN ADMINISTRATIVA." Revista de Derecho de la Universidad de Montevideo. Diciembre 2012. Pág. 132.

[8] DURAN MARTINEZ, Augusto. Seminario. "Neoconstitucionalismo. Límites constitucionales al poder político". http://www.institutomanueloribe.com.uy/contenido/Neoconstitucionalismo. Acc. 28/8/2016.

[9] Disponible en http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/C43D4582907B58900525780800763C5A/$FILE/nahabetian.pdf. Ult. Acc. 25/08/2016.

[10] En "El principio de proporcionalidad y la interpretación constitucional". Ministerio de Justicia y Derechos Humanos. Disponible en: http://www.biblio.dpp.cl/biblio/DataBank/4271.pdf. Ult. acceso: 26/08/2016.

Informe Nº 395/019, de 22 de octubre de 2019

Se resuelve una denuncia sobre el presunto incumplimiento de los plazos para habilitar el ejercicio de los derechos consagrados en la Ley N° 18.331.

Montevideo, 22 de octubre de 2019

Exp. 2019-2-10-0000393

Denuncia Sr. AA contra BANCO SANTANDER por envío de publicidad sin consentimiento del titular

Informe N° 395

I.- Antecedentes

Con fecha 18 de setiembre de 2019, se recibe denuncia del Sr. AA quien manifiesta que:

“Desde 2015 solicito no recibir más mails por parte del Banco Santander S.A., ya que no soy más cliente desde ese año. Luego de avisar reiteradas veces (primera solicitud de baja en 2015) y sin embargo seguir recibiendo mails promocionales, hago la denuncia por violación del artículo 14 de la Ley 18.331. Además, no sé si el banco manda los mails, o si terceriza el envío y otra empresa más tiene mis datos. Desde que resido en la Unión Europea, si la ley 18.331 no me amparase, me ampara el Reglamento General de Protección de Datos (GDPR) (Reglamento 2016/679), sancionando con multas del 2-4% del ingreso mundial anual de la empresa o 10-20 millones de Euros. Prefiero iniciar el trámite en Uruguay ya que el banco está en falta ahí.”

Adjunta documentación -identificada en Anexos 1, 2 y 3- en las cuales adjunta copia de los correos electrónicos recibidos, así como copia de los 9correos solicitando la supresión de los datos.

Se dio vista a BANCO SANTANDER con fecha 23 de setiembre de 2019.

BANCO SANTANDER evacuó vista con fecha 10 de octubre de 2019.

En la misma manifestó que lamenta las molestas ocasionadas y que procederá a tomar las medidas pertinentes para evitar futuros casos como el presente y cumplir con lo solicitado por el denunciante. Argumenta que lo sucedido es un error humano al momento de efectuar la marca de no contactibilidad.

Asimismo manifiesta que ante la constatación de este error humano, se procederá a tomar las medidas necesarias para evitar que el cliente continúe recibiendo correos promocionales, por lo que no debería volver a recibir mensajes promocionales por parte de Banco Santander.

II.- Informe jurídico

De lo que surge del expediente en análisis se desprende que se ha formulado denuncia por parte del Sr. AA ante esta Unidad en base a un eventual incumplimiento del art. 15 de la Ley de Protección de Datos Personales, art. 21 de la misma Ley y art. 13 del Decreto reglamentario N° 414/009.

Habiéndose dado vista de la denuncia formulada a la denunciada y de acuerdo a lo informado por la misma surge que efectivamente hubo un incumplimiento del art. 15 y 21 de la Ley N° 18.331 y art. 13 del Decreto N° 414/009, en cuanto la empresa no cumplió con el debido procedimiento establecido por la Ley de Protección de Datos Personales ante una solicitud de supresión realizada por un titular.

El art. 15 establece que: “El responsable de la base de datos o del tratamiento deberá proceder a realizar la rectificación, actualización, inclusión, o supresión mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar las razones por las que estime no corresponde.”

Asimismo el art. 13 del Decreto reglamentario establece que: “El derecho de supresión es el que tiene el titular a que se eliminen los datos cuya utilización por terceros resulte ilegítima, o que resulten ser inadecuados o excesivos.”

Por su parte el art. 21 de la Ley N° 18.331 establece que: “(Datos relativos a bases de datos con fines de publicidad).- En la recopilación de domicilios, reparto de documentos, publicidad, prospección comercial, 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.

En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno. El titular 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.”

Dado lo que expresa la normativa vigente, se ha producido un incumplimiento por parte del responsable de la base de datos, no habiendo brindado el derecho de supresión que le fuere repetidamente solicitado por el titular del dato, en clara violación de los preceptos legales.

Asimismo deja en evidencia que su base de datos se encuentra desactualizada, no expresando cómo es que se efectuará dicho procedimiento de supresión. Por lo tanto, tampoco accede a la supresión inmediata y no expresa el mecanismo que se realizará para verificar con veracidad que dicho dato fue suprimido de su o sus bases de datos, tal como lo solicita el titular, más aún teniendo presente el plazo de 5 días hábiles que la ley le concede para efectuar dicha supresión.

Debido a lo anterior es que se constata el incumplimiento por parte de BANCO SANTANDER.

III.- Conclusiones

Dado lo expresado anteriormente, esta informante sugiere:

Recomendar al Consejo Ejecutivo de esta Unidad imponga la sanción que corresponda en el caso concreto a BANCO SANTANDER S.A. por incumplir con el derecho de supresión solicitado por el denunciante.

Recomendar al Consejo Ejecutivo de esta Unidad intimar a BANCO SANTANDER a que acredite cuál sería el procedimiento de supresión empleado en el caso y acreditar que efectivamente se procedió a suprimir dichos datos en el plazo de 5 días hábiles.

Es todo cuanto tengo que informar.

Dra. Esc. Lylian Massarino

Informe Nº 412/019, de 31 de octubre de 2019

Se informa una consulta formulada por la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo (SENACLAFT) respecto a una intimación de entrega de copia de resoluciones que aplican sanciones a los sujetos obligados no financieros remitida por el Tribunal de lo Contencioso Administrativo, a requerimiento de la parte actora en un juicio en que la Secretaría es demandada.

Montevideo, 1° de noviembre de 2019

Exp. 2019- 448

Consulta de la Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo sobre resoluciones solicitadas por el TCA

Informe N° 412

I.- La consulta

Se presenta ante esta Unidad la Secretaría nacional para la lucha contra el lavado de activos y el financiamiento del terrorismo (en adelante SENACLAFT) para pedir opinión respecto a una solicitud recibida. Se indica que el Tribunal de lo Contencioso Administrativo, a solicitud de la parte actora, en un juicio en que la Secretaría es demandada, ha intimado agregar la copia de la totalidad de las resoluciones que aplican sanciones a los sujetos obligados no financieros.

Expresan que las referidas resoluciones contienen datos personales tanto de los sujetos obligados (nombres y documentos) como de sus clientes, y que en consecuencia, y si bien entienden que dichos datos deben ser protegidos al amparo de la normativa vigente lo que impediría cumplir con la intimación efectuada, se considera oportuno recabar la opinión de esta Unidad.

II – Análisis

Conforme con la información brindada, estamos ante la presencia de una comunicación de datos desde una perspectiva de protección de datos personales. En ese sentido, el artículo 4° literal b) de la Ley N° 18.331, de 11 de agosto de 2008, considera que la comunicación de datos es "*toda revelación de datos realizada a una persona distinta de titular de datos".* Por su parte, el artículo 17 de la citada norma establece los requisitos necesarios para su realización. En efecto, esta última norma edicta que sólo podrán ser comunicados los datos personales 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, estableciendo esta misma norma los casos en los cuáles se puede excepcionar de consentimiento.

Este artículo establece que el previo consentimiento no será necesario cuando A) así lo disponga una ley de interés general. B) en los supuestos del artículo 9° de la presente ley. C) 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. D) se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables. Además agrega que el destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

Cabe indicar además que en relación con el literal B) citado, los supuestos del artículo 9° de la ley son los siguientes: a) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación, b) se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, c) se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma, d) deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento, e) se realice por personas físicas para su uso exclusivo personal, individual o doméstico.

Además, por su parte, el art. 9 – BIS de la Ley N° 18.331, de 11 de agosto de 2008, establece cuáles son las fuentes públicas o accesibles al público

Finalmente, y a efectos de tomar en cuenta todo el marco normativo aplicable, es necesario considerar que el art. 18 de la LPDP establece que: *"Los datos relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas, sin perjuicio de las autorizaciones que la ley otorga u otorgare. Nada de lo establecido en esta ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren inconveniente"*.

Teniendo en consideración las normas citadas ut supra, corresponde analizar si se cumplen con los requisitos para establecer si la SENACLAFT debe entregar la información solicitada. A esos efectos, se considera necesario analizar las competencias de ésta. En este sentido, el artículo 4 de la Ley N° 19.574, de 20 de diciembre de 2017, expresa que "…*La Secretaría Nacional para la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo, como órgano desconcentrado dependiente directamente de la Presidencia de la República, diseñará las líneas generales de acción para la lucha contra el lavado de activos y el financiamiento del terrorismo. La misma actuará con autonomía técnica, y tendrá los siguientes cometidos: (…) E) El control del cumplimiento de las normas de prevención de lavado de activos y financiamiento del terrorismo por parte de los sujetos obligados por el artículo 13 de la presente ley. (…) H) Ejecutar las sanciones pecuniarias que imponga mediante resolución…".*

Por tanto, la solicitud es realizada a la Entidad Pública competente para brindar la información solicitada. En cuanto al interés del destinatario ha sido opinión firme de esta Unidad, que cuando la información sea solicitada en el marco de una función jurisdiccional, ésta debe ser entregada. Por ejemplo, en el Dictamen N° 10/019, 27 de agosto de 2019, esta Unidad ha entendido que en materia de juzgados *"En consecuencia, si existe un interés por parte del Juzgado correspondiente, reflejado en un oficio, con determinación de la información solicitada, su fin y aplicación a un proceso determinado, corresponderá su entrega".*

En cuanto a la necesidad del previo consentimiento informado de los titulares de datos, corresponde indicar que al caso concreto se aplica el artículo 9° literal b) de la Ley N° 18.331, de 11 de agosto de 2008, por lo que no resulta necesario recabarlo en tanto nos encontramos ante una Entidad Pública en ejercicio de sus funciones y se trata de una obligación legal.

En virtud de lo expuesto, esta informante entiende que se encuentran debidamente acreditados todos los requisitos del artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008, para proceder a entregar la información solicitada.

A mayor abundamiento, también esta Unidad se ha pronunciado sobre otra consulta de esta misma Entidad relacionada con la publicación de Resoluciones. Es así que mediante Dictamen N° 11/019, se ha indicado que "*III. Que además, todo tratamiento de datos, incluyendo su comunicación, deberá ajustarse a los principios establecidos en la Ley N° 18.331, sin perjuicio de la clasificación o calificación que se realice por parte de SENACLAFT de la información contenida en el expediente en el marco de lo dispuesto en la Ley N° 18.381, de 17 de octubre de 2018".*

III.- Conclusiones

De acuerdo con lo informado, se considera que la SENACLAFT debe proceder a entregar la información solicitada en virtud de que, desde el punto de vista de protección de datos personales, se cumplen con todos los requisitos necesarios para realizar la citada comunicación de datos personales.

Es todo cuanto tengo que informar.

Dra. Flavia Baladán

Informe S/N, de 9 de setiembre de 2019

Se resuelve analizar un oficio respecto al tratamiento de los datos personales en dos organismos del Estado.

Expediente 2019-2-10-0000180

Montevideo, 9 de setiembre de 2019

Informe N° S/N

-ANTECEDENTES-

Vienen los presentes atento a las actuaciones llevadas delante de oficio, y a denuncia de parte, respecto a la conformación de una base de datos en la que se incluyen todas las cédulas de identidad de uruguayos, obtenidas conforme se indica en la página web que surge de obrados, de distintas fuentes disponibles en internet.

Se señala en la citada página que esta Unidad se ha pronunciado en forma favorable a esta base, lo que de plano se descarta, lo que además se fundamenta en lo que se dirá a continuación.

-EL ANÁLISIS DEL CASO CONCRETO-

La situación puntualmente refiere a la publicación en forma libre, y por parte de un particular, de una lista completa de cédulas de identidad asociadas a nombres y apellidos.

Tratándose de una base de datos, y de información que contiene datos personales de los involucrados, corresponde determinar si es posible su comunicación en la forma planteada, debiendo tener presente dos cuestiones: en primer lugar, si la información contenida en la base de datos es pública en los términos de la Ley N° 18.331, y en segundo lugar, aun tratándose de información pública, si corresponde su entrega en la forma peticionada.

El artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008 edicta 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, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.*

El previo consentimiento para la comunicación es revocable.

El previo consentimiento no será necesario cuando:

A) así lo disponga una ley de interés general.

B) en los supuestos del artículo 9° de la presente ley.

C) 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.

D) se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate".

Por su parte el artículo 9° 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.*

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 13 de la presente ley.

No será necesario el previo consentimiento cuando:

A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.

B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

E) Se realice por personas físicas para su uso exclusivo personal, individual o doméstico."

En lo que refiere a las fuentes públicas de información, el artículo 9° bis de la citada Ley indica que son públicas o accesibles al público: "*A) El Diario Oficial y las publicaciones oficiales, cualquiera sea su soporte de registro o canal de comunicación.*

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

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

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

En este sentido, debe tenerse en cuenta que toda comunicación de datos personales debe hacerse considerando el interés legítimo del emisor y del destinatario de los datos. Esta previsión, incluida en el artículo 17, es adicional al consentimiento o de sus excepciones, y se constituye en un requisito indispensable para habilitar toda comunicación de datos.

Por ende, el hecho de que el artículo 9° de la ley en su literal C habilite el tratamiento de datos, en el caso no existe un interés legítimo comprobable del destinatario que habilite dicha comunicación.

Pero además, el tratamiento de datos personales requiere el cumplimiento de los otros principios explicitados en la Ley. En particular el principio de finalidad (Artículo 8°) indica que: *"Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.*

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

La reglamentación determinará los casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aún cuando haya perimido tal necesidad o pertinencia.

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

La finalidad de los datos personales contenidos en las bases de datos de la DNIC se encuentra reglada por varias normas entre las que se encuentra el artículo 21 del decreto-Ley N° 14.762 de 13 de febrero de 1979, y su tratamiento autorizado en especial por el artículo 151 de la Ley N° 16.736, de 5 de enero de 1996, y 81 de la Ley N° 16.462, de 11 de enero de 1994, además de las reglamentaciones pertinentes. En este caso puntual, no

se observa una finalidad compatible o similar a la indicada para los datos contenidos en las bases de DNIC.

Además, el tratamiento en general de esta nueva base generada se encuentra permeado de una notoria ilicitud, al no encontrarse la misma inscripta, vulnerando en definitiva el artículo 6 de la Ley N° 18.331.

Y ello sin perjuicio de la ilicitud derivada de la inexistencia de mecanismos que habiliten el cumplimiento de los derechos por parte de los titulares de los datos personales, de conformidad con lo establecido en los artículos 14 y siguientes de la Ley N° 18.331, y la inexistencia de una autorización particular o de una acreditación fehaciente de la ubicación precisa del servidor donde se encuentran alojados los datos, a efectos de comprobar el cumplimiento o no de lo indicado en el artículo 23 de la Ley mencionada.

Con respecto a los listados de credenciales cívicas, son aplicables in totum las consideraciones arriba vertidas, debiendo considerar al respecto además la Ley N° 7.812 de 16 de enero de 1925, en la redacción dada por las Leyes N° 17.113, de 9 de junio de 1999 y 17.239, de 2 de mayo de 2000.

Por lo antedicho, se sugiere intimar a que en forma inmediata se den de baja los archivos referidos en la página denunciada y se de vista de estas actuaciones y de lo informado al Señor AA en AAA@AAA.com a efectos de que se pronuncie con respecto a lo indicado en este informe.

Es cuanto tengo para informar.

Dr. Gonzalo Sosa

Resoluciones

Resolución Nº 2/019, de 15 de enero de 2019. Se resuelve una denuncia sobre el incumplimiento del derecho de acceso al no entregar los datos solicitados en el plazo establecido por la norma.

Resolución Nº 4/019, de 12 de marzo de 2019. Se resuelve actualizar la Resolución N° 17/009, de 12 de junio de 2009, sobre los países u organizaciones consideradas adecuadas para las transferencias internacionales de datos, de conformidad con lo establecido por el artículo 23 de la Ley N° 18.331, de 11 de agosto de 2008.

Resolución Nº 7/019, de 26 de marzo de 2019. Se resuelve una denuncia acerca de la recepción de mensajes por parte de una empresa con la que el denunciante nunca operó.

Resolución Nº 9/019, de 26 de marzo de 2019. Se resuelve una denuncia vinculada con la instalación de cámaras de videovigilancia en una copropiedad en presunta infracción a la normativa de protección de datos personales.

Resolución Nº 11/019, de 2 de abril de 2019. Se resuelve una denuncia sobre el presunto incumplimiento de los plazos para habilitar el ejercicio de los derechos consagrados en la Ley N° 18.331.

Resolución Nº 13/019, de 23 de abril de 2018. Se resuelve una denuncia referente a la instalación de varias cámaras de videovigilancia a través de las que se filma la vía pública y los frentes de las viviendas.

Resolución Nº 15/019, de 23 de abril de 2019. Se resuelve una denuncia relacionada con la publicación de un listado de estudiantes sin su consentimiento en una plataforma universitaria.

Resolución Nº 21/019, de 14 de mayo de 2019. Se autoriza la transferencia internacional de datos presentada por Centro Ceibal para el Apoyo a la Educación de la Niñez y la Adolescencia.

Resolución Nº 22/019, de 14 de mayo de 2019. Se resuelve sobre la denuncia presentada contra una empresa en relación con la comunicación de datos personales a terceros.

Resolución Nº 25/019, de 28 de mayo de 2019. Se resuelve una denuncia por publicación en Internet de certificados médicos de una trabajadora luego de culminada su relación laboral.

Resolución Nº 27/019, de 28 de mayo de 2019. Se resuelve una denuncia en relación con la instalación de una cámara de videovigilancia en posible infracción a los requerimientos de protección de datos personales.

Resolución Nº 28/019, de 28 de mayo de 2019. Se resuelve una denuncia contra un banco de plaza por errónea calificación y no actualización de datos personales del denunciante.

Resolución Nº 29/019, de 28 de mayo de 2019. Se resuelve una denuncia por utilización sin consentimiento de la imagen del denunciante.

Resolución Nº 31/019, de 2 de julio de 2019. Se resuelve una denuncia referida a la utilización de datos personales sin el previo consentimiento de su titular.

Resolución Nº 33/019, de 2 de julio de 2019. Se resuelve una denuncia por presunto incumplimiento del derecho de supresión.

Resolución Nº 36/019, de 13 de agosto de 2019. Se resuelve una denuncia referida a la utilización de datos diferentes a los que se habían proporcionado.

Resolución Nº 37/019, de 13 de agosto de 2019. Se resuelve una denuncia referida a la comunicación de datos personales sin consentimiento.

Resolución Nº 43/019, de 24 de setiembre de 2019. Se resuelve una denuncia referida al presunto incumplimiento del derecho de supresión.

Resolución Nº 44/019, de 24 de setiembre de 2019. Se resuelve una denuncia referida al incumplimiento del derecho de supresión.

Resolución Nº 45/019, de 24 de setiembre de 2019. Se resuelve un oficio respecto al tratamiento de datos personales en dos organismos del Estado.

Resolución Nº 46/019, de 1 de octubre de 2019. Se resuelve una denuncia referida a la presunta falta de respuesta ante el ejercicio del derecho de acceso.

Resolución N° 48/019, de 22 de noviembre de 2019. Se resuelve una denuncia referida a la incorporación indebida del denunciante a un bureau de crédito por parte de la empresa denunciada.

Resolución Nº 2/019, de 15 de enero de 2019

Se resuelve una denuncia sobre el incumplimiento del derecho de acceso al no entregar los datos solicitados en el plazo establecido por la norma.

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

RESOLUCIÓN N°	2	2019
EXPEDIENTE N°	2018-2-10-0000119	

Montevideo, 15 de enero de 2019

VISTO: La denuncia formulada por la señora Mary Karina Olivera Lemes contra la empresa Pronto!

RESULTANDO:

1. Que la denuncia versa sobre el incumplimiento del derecho de acceso, debido a que con fecha 6 de febrero de 2018 presentó formulario para el ejercicio del derecho indicando que la empresa denunciada no cumplió con la entrega solicitada.
2. Que Bautzen SA y Kedal SA expresan que el 29 de enero del 2018 se emitieron por Bautzen SA, dos órdenes de compra a nombre de la Sra. Mary Karina Olivera Lemes en un local de “Da Pie Pro Sport”. En el mismo día se habrían comunicado con la Sra. Olivera para darle la bienvenida a Pronto!, quien manifiesta el desconocimiento de las mencionadas órdenes de compra, recomendándole realice reclamo formal, lo que se efectúa con fecha 30 de enero.
3. Que indica la parte denunciada que con fecha 6 de febrero de 2018 la Sra. Olivera presentó formulario para ejercer el derecho de acceso a sus datos personales, procediendo Pronto! a incluir estas actuaciones en el reclamo formal antes reseñado.
4. Que de los descargos presentados por Pronto! surge que la Sra. Olivera no solo ejerció su derecho de acceso sino que además, ante el transcurso del plazo presentó denuncia a nivel policial (14/02/2018) y ante el Defensor del Cliente de Pronto (14/02/2018). Según se indica en el punto V) del escrito mencionado, el día 21 de febrero se le envió correo electrónico a la Sra. Olivera confirmándole los datos personales que figuraban en la base de datos de Pronto, verificándose incumplimiento del plazo legal y de lo solicitado por la denunciante.
5. Que Kedal SA carece de legitimación pasiva debido a que las órdenes de compra fueron emitidas respecto de la empresa Bautzen SA.

CONSIDERANDO:

1. Que resulta de plena aplicación al caso, el artículo 14 de la Ley N° 18.331 de 11 de agosto de 2008, por el que se establece que el 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.
2. Que el mencionado artículo indica que la información debe ser proporcionada dentro de los cinco días hábiles de haber sido solicitada

ATENTO: A lo expuesto e informado,

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

Personales

RESUELVE

1. Sancionar a Bautzen SA con apercibimiento por haber incumplido con las disposiciones de la Ley N° 18.331 de 11 de agosto de 2008, en particular el artículo 14, en cuanto excedió el plazo legal de 5 días hábiles para otorgar acceso a sus datos personales a la Sra. Olivera.
2. Indicar que procede el archivo sin perjuicio de estas actuaciones respecto a la empresa Kedal SA, por carecer de legitimación pasiva.
3. *Notifíquese, publíquese y oportunamente archívese.*

DR. FELIPE ROTONDO

URCDP

Resolución Nº 4/019, de 12 de marzo de 2019

Se resuelve actualizar la Resolución N° 17/009, de 12 de junio de 2009, sobre los países u organizaciones consideradas adecuadas para las transferencias internacionales de datos, de conformidad con lo establecido por el artículo 23 de la Ley N° 18.331, de 11 de agosto de 2008.

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

RESOLUCIÓN N°	4	2019
ACTA N°	3	2019

Montevideo, 12 de marzo de 2019

VISTO: La necesidad de actualizar la Resolución Nº 17/009, de 12 de junio de 2009, sobre los países u organizaciones consideradas adecuadas para las transferencias internacionales de datos, de conformidad con lo establecido por el artículo 23 de la Ley Nº 18.331, de 11 de agosto de 2008.

RESULTANDO:

1. Que como se establece en la citada Resolución, la transferencia internacional de datos supone su transmisión fuera del territorio nacional, y se constituye una cesión o comunicación que tiene por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo.
2. Que la misma Resolución prevé como países apropiados para las transferencias internacionales de datos, los que a juicio de esta Unidad, cuenten con normas de protección adecuadas y medios para asegurar su aplicación eficaz, encontrándose comprendidos los países miembros de la Unión Europea y aquellos que la Comisión Europea considere garantizan las condiciones antes indicadas.
3. Que, en función de la Resolución antedicha, se presenta el Departamento de Servicios Digitales, Cultura, Medios y Deporte del Reino Unido de Gran Bretaña e Irlanda del Norte a efectos de que se le considere adecuado para las transferencias internacionales, considerando que a partir del 29 de los corrientes mes y año dejará de formar parte de la Unión Europea. Adjunta documentación que fue debidamente analizada e informada, considerándose apropiado acceder a lo solicitado.

CONSIDERANDO:

1. Que el artículo 23 de la Ley Nº 18.331 dispone la prohibición de transferencias internacionales de datos con países u organismos internacionales que no proporcionen niveles de protección adecuados, de acuerdo con los estándares del Derecho Internacional o Regional en la materia, salvo excepciones.
2. Que esta Unidad es el órgano encargado de establecer las condiciones y analizar la procedencia de las solicitudes de adecuación de terceros países, en función de la normativa citada.
3. Que en la situación actual de la materia corresponde atender –entre otros documentos- los Estándares Iberoamericanos de Protección de Datos Personales emitidos por la Red Iberoamericana de Protección de Datos y el Reglamento General Europeo de Protección de Datos Nº 2016/679 del Parlamento Europeo y del Consejo.
4. Que, en ese sentido, los países miembros de la Unión Europea cumplen con los estándares internacionales desde que el Reglamento les es aplicable en forma directa, mientras que las decisiones de adecuación adoptadas por la Comisión Europea para terceros países permiten considerar que esos países poseen un nivel adecuado de protección, por acompasar su normativa interna a la de dicho estándar internacional.
5. Que, sin perjuicio de lo mencionado en el apartado anterior, en el caso de terceros países u organizaciones considerados adecuados por la Comisión Europea, deberán entenderse incluidas en la presente Resolución todas las limitaciones o excepciones previstas en la decisión correspondiente.

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

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE

1. Sustituir la Resolución Nº 17/009, de 12 de junio de 2009, y establecer que se consideran adecuados y en consecuencia apropiados para las transferencias internacionales de datos, todos los países que a juicio de esta Unidad, cuenten con normas de protección adecuadas y medios para asegurar su aplicación eficaz. En particular, se consideran adecuados a los miembros de la Unión Europea y el Espacio Económico Europeo, Principado de Andorra, República Argentina, el sector privado de Canadá, las organizaciones incluidas en el marco “Privacy Shield” de los Estados Unidos de América, Guernsey, Isla de Man, Islas Feroe, Estado de Israel, Japón, Jersey, Nueva Zelanda, Reino Unido de Gran Bretaña e Irlanda del Norte, y Confederación Suiza.
2. La realización de las transferencias a los países indicados en el numeral anterior se encontrará supeditada, en caso de corresponder, a lo referido en el Considerando V de esta Resolución.

3. Notifíquese, publíquese y oportunamente archívese.

DR. FELIPE ROTONDO

URCDP

Resolución Nº 7/019, de 26 de marzo de 2019

Se resuelve una denuncia acerca de la recepción de mensajes por parte de una empresa con la que el denunciante nunca operó.

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

RESOLUCIÓN N°	7	2019
Expediente N°	2018-2-10-0000519	

Montevideo, 26 de marzo de 2019

VISTO: La denuncia presentada por el Sr. AA contra DISTRICOMP S.A. por correo electrónico no deseado o spam.

RESULTANDO:

1. Que el denunciado manifiesta haber recibido correos no deseados de la denunciada, pese a su manifestación en contrario vía correo electrónico su deseo en contrario y habérsele confirmado la supresión de sus datos de la base de la denunciada.
2. Que se le dio vista a la denunciada, la que manifiesta que por error se suprimió de la base de datos a otro cliente homónimo del denunciante, razón por la cual le sigue llegando publicidad no deseada.
3. Que pese a que la denunciada no contaba con bases inscriptas, las presentó para su inscripción luego de notificado por esta Unidad.

CONSIDERANDO:

1. Que el artículo 15° de la Ley N° 18.331, de 11 de agosto de 2008 establece las condiciones y supuestos para el ejercicio del derecho de supresión. La citada norma debe complementarse con lo establecido por el artículo 21° de la Ley, para el caso de envío de publicidad no deseada.
2. Que en el presente caso se ha acreditado por la denunciada que existió un error a la hora de proceder a la supresión de la información, y que enterada del caso efectuó las correcciones pertinentes.

ATENTO: A lo expuesto,

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

RESUELVE:

1. *Hacer saber* a DISTRICOMP S.A. que deberá adecuar sus procesos internos a efectos de evitar situaciones que impidan a los titulares de los datos, un adecuado ejercicio de los derechos consagrados por la Ley N° 18.331, de 11 de agosto de 2018.
2. *Notifíquese, publíquese y oportunamente archívese.*

DR. FELIPE ROTONDO

URCDP

Resolución Nº 9/019, de 26 de marzo de 2019

Se resuelve una denuncia vinculada con la instalación de cámaras de videovigilancia en una copropiedad en presunta infracción a la normativa de protección de datos personales.

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

RESOLUCIÓN N°	9	2019
Expediente N°	2017-2-10-000550	

Montevideo, 26 de marzo de 2019

VISTO: La denuncia realizada por la instalación de cámaras de video-vigilancia en una copropiedad en presunta infracción a la normativa de protección de datos personales.

RESULTANDO:

1. Que de la denuncia se procedió a dar vista al denunciado, quien expresó que los hechos expresados eran falsos, que las cámaras exclusivamente apuntan hacia los espacios comunes, que la decisión fue adoptada en común acuerdo entre los copropietarios y que las cámaras están señalizadas, solicitándose inspección de tales extremos.
2. Que el 12 de marzo se realizó la inspección solicitada, y se procedió a dar vista a las partes, quiénes la evacuaron en tiempo y forma.

CONSIDERANDO:

- I. Que el presente caso versa sobre la instalación de cámaras de video-vigilancia en una propiedad horizontal resultando de lo dispuesto en la Ley N° 18.331, de 11 de agosto de 2008.
- II. Que por Dictamen N° 10/010, de 16 de abril de 2010, este Consejo Ejecutivo definió a la video-vigilancia como *"toda grabación, captación, transmisión, conservación y almacenamiento de imágenes, y en algunos casos de sonidos, mediante la utilización de videocámaras u otros medios análogos*" y precisó el régimen aplicable a su respecto. Por Resolución N° 989/010, de 30 de julio de 2010, se estableció la necesidad de contar con logos de video-vigilancia.
- III. Que la Guía de video-vigilancia en edificios, complejos y cooperativas de la URCDP, indica que *"Las cámaras que se utilicen solo podrán enfocar los espacios comunes y que sean considerados de vigilancia necesaria. En el caso de los edificios, se consideran espacios comunes las escaleras, los ascensores, el hall de entrada, los pasillos y cualquier otro determinado por el reglamento de copropiedad, siempre teniendo presente que el número de cámaras no debe ser desproporcionado al área que se vigilará".*
- IV. Que en el presente caso se constata la existencia de una cámara que apunta más allá del hall de entrada de la propiedad, captando incluso parte de la calle como se constata con la foto de fs. 50. Además, una de las cámaras del corredor capta parte de patio de la denunciante, todo lo cual resulta desproporcionado y vulnera el principio de finalidad.
- V. Que a ello se agrega que no se constata la inscripción de las bases de datos así como tampoco el uso de logos de videovigilancia y que el acuerdo de la copropiedad fue realizado con posterioridad a la denuncia presentada ante esta Unidad.

ATENTO: a lo expuesto,

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

RESUELVE:

1. Intimar a los AA, la desinstalación de la cámara que apunta hacia la calle y la corrección del ángulo de la cámara que apunta al patio de la denunciante, debiendo demostrar su cumplimiento en un plazo de 30 días, bajo apercibimiento.
2. Intimar la inscripción de la base de datos y la incorporación de logos de video-vigilancia en el mismo plazo, bajo apercibimiento.
3. Notifíquese y publíquese.

DR. FELIPE ROTONDO

URCDP

Resolución Nº 11/019, de 2 de abril de 2019

Se resuelve una denuncia sobre el presunto incumplimiento de los plazos para habilitar el ejercicio de los derechos consagrados en la Ley N° 18.331.

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

RESOLUCIÓN N°	11	2019
Expediente N°	2018-2-10-000393	

Montevideo, 2 de abril de 2019

VISTO: La denuncia presentada por el señor AA contra la empresa OVATSOL S.A.

RESULTANDO:

1. Que el denunciante indica que la denunciada expuso datos personales de sus clientes, específicamente nombres, teléfonos, correos electrónicos, cédulas de identidad, direcciones y firmas, todo a través de su sitio web. Manifiesta además que se puede acceder a información personal a través de una dirección que no controla si el usuario está logueado en la página, y que si se cambia el parámetro, se accede a información de cada uno de sus clientes. Expresa que informó oportunamente a la empresa.
2. Que el 10 de agosto de 2018 se realizó comprobación del sitio web de la denunciada, sin que se hubieran podido confirmar los dichos del denunciante.
3. Que con fecha 5 de setiembre de 2018 se dio vista a la denunciada y en su evacuación de vista expresa que recibió el aviso del denunciante y en ese marco le solicitaron más información, sin perjuicio de lo cual al día siguiente resolvieron la situación y lo informaron el denunciante.

CONSIDERANDO:

1. Que el presente caso refiere a una vulneración de seguridad por la que se posibilitó en forma involuntaria el acceso a datos personales tales como nombres, teléfonos, correos electrónicos, cédulas de identidad, direcciones y firmas, siendo de aplicación lo dispuesto en la Ley N° 18.331, de 11 de agosto de 2008.
2. Que lo sucedido se enmarca en una vulneración del principio de seguridad regulado en el artículo 10 de la citada norma, reglamentado por los artículos 7 y 8 del Decreto 414/009, de 31 de agosto de 2009.
3. Que se debe tener presente que advertida de la situación, la empresa adoptó las medidas necesarias para resolverla, y recaudos para evitar futuras vulneraciones a la base de datos. No se ha constatado por otra parte, la existencia de perjuicios a terceros.
4. Que a la fecha no surgen bases de datos inscriptas a nombre de la denunciada.

ATENTO: a lo expuesto,

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

RESUELVE:

1. Apercibir a OVATSOL S.A. por vulnerar el principio de seguridad consagrado en el artículo 10 de la Ley N° 18.331, de 11 de agosto de 2008.
2. Intimar a OVATSOL S.A. la inscripción de todas sus bases de datos en un plazo de 30 días corridos, bajo apercibimiento.
3. Notifíquese, publíquese y oportunamente archívese.

DR. FELIPE ROTONDO

URCDP

Resolución Nº 13/019, de 23 de abril de 2018

Se resuelve una denuncia referente a la instalación de varias cámaras de videovigilancia a través de las que se filma la vía pública y los frentes de las viviendas.

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

RESOLUCIÓN N°	13	2019
Expediente N°	2018-2-10-000296	

Montevideo, 23 de abril de 2019

VISTO: La denuncia realizada en relación con la instalación de varias cámaras de videovigilancia a través de las cuáles se filma la vía pública y los frentes de las viviendas.

RESULTANDO:

1. Que el denunciante indica que se encuentran cuatro cámaras en una acera y cuatro en la otra, filmando cada una hacia la acera del frente, pudiendo filmar incluso lo que sucede en el interior de las viviendas. Las imágenes son difundidas por Internet a efectos de que algunos vecinos dispongan de acceso a éstas.
2. Que se obtuvo información respecto del titular de la dirección denunciada, y se procedió a dar vista, la que fue evacuada expresando que la instalación de cámaras es una iniciativa de seguridad promovida por la mayoría de las familias residentes en esa zona de la ciudad. Además, cuentan con un grupo de Whatsapp, cartelería de vecinos en alerta, reuniones de análisis de proyectos, todo ello con la finalidad de combatir la inseguridad. Las cámaras fueron financiadas en forma colaborativa por los vecinos y la instalación fue de su cargo. Mencionan que están en contacto con el Ministerio del Interior a efectos de iniciar acciones colectivas y ante el reclamo concreto, han implementado una prestación del sistema por medio de la cual se bloquea la visión de una zona de la imagen logrando evitar la captación de imágenes de la vivienda del denunciante.
3. Que se procedió a dar vista al denunciante para que expresara su conformidad o no con la solución propuesta por los denunciados, quien expresó que no posee control sobre las imágenes por lo que se ve impedido de corroborarla. Indica que previo a la denuncia se le había expresado que su vivienda no iba a ser captada por las imágenes, no siendo así en los hechos, entre otros alegatos.
4. Que, en forma complementaria, se procedió a dar vista a la Dirección General de Fiscalización de Empresas del Ministerio del Interior, expresando ésta que no habilita cámaras ni sistemas de cámaras (sean individuales o barriales) así como tampoco está a su cargo el contralor de la disposición de las cámaras de seguridad, los registros fílmicos, entre otros.

CONSIDERANDO:

1. Que las imágenes y sonidos captadas por cámaras son datos personales de conformidad con la definición del artículo 4° literal d) de la Ley N° 18.331, de 11 de agosto de 2008.
2. Que por Dictamen N° 10/010, de 16 de abril de 2010, se definió la videovigilancia y estableció cómo se pueden utilizar estos sistemas –que por definición son subsidiarios y solamente pueden utilizarse cuando no existen otros medios menos lesivos de la intimidad de las personas-, los principios aplicables, si procede el registro de base de datos personales, y los casos en que no es aplicable la normativa de protección de datos. En cuanto a la necesidad de contar con logos de videovigilancia, cabe indicar que su patrón fue aprobado por Resolución de este Consejo N° 989/010, de 30 de julio de 2010.
3. Que la función de seguridad del espacio público corresponde en exclusividad al Ministerio del Interior, en ejercicio de sus competencias. En ese marco, según el Diccionario de la Real Academia Español éste se define como "*1. f. Calle, plaza, camino u otro sitio por donde transita o circula el público" y s*obre este punto la Agencia Española de Protección de Datos en su Resolución R/02340/2012 se remite a la definición citada a la cual agrega que "…*debe insistirse en que la titularidad privada de un terreno abierto no justifica per se la realización de grabaciones de imágenes en el caso de que se trate de un "lugar público".*
4. Que en determinados casos resulta imprescindible captar parte de la vía pública para la finalidad de vigilancia que se pretende realizar, siguiendo el principio consagrado por el artículo 8° de la Ley N° 18.331, de 11 de agosto de 2008.
5. Que, no obstante, no debe olvidarse que con la intención de lograr mayor seguridad se pueden llegar a adoptar medidas restrictivas de derechos fundamentales como lo es el derecho a la intimidad. Por tanto, la videovigilancia debe ser una medida adecuada, pertinente y no excesiva en relación con la finalidad perseguida, y se debe analizar si la finalidad de seguridad no puede alcanzarse por otros medios alternativos, menos intrusivos para el derecho a la protección de datos personales.

ATENTO: a lo expuesto e informado,

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

RESUELVE:

1. Intimar a los denunciados a adoptar todas las medidas necesarias para no captar imágenes relacionadas con la vivienda del denunciante, por no ajustarse la solución puesta en práctica por éstos a la normativa en materia de protección de datos personales, dando cuenta a esta Unidad en el plazo de 30 días corridos a contar de la notificación.
2. Intimar a los denunciados a adoptar los logos recomendados por esta Unidad y a registrar las bases si estas graban las imágenes aún por períodos breves, dando cuenta a esta Unidad en el plazo de 30 días corridos a contar de la notificación.
3. NOTIFÍQUESE Y PUBLÍQUESE

DR. FELIPE ROTONDO

URCDP

Resolución Nº 15/019, de 23 de abril de 2019

Se resuelve una denuncia relacionada con la publicación de un listado de estudiantes sin su consentimiento en una plataforma universitaria.

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

RESOLUCIÓN N°	15	2019
Expediente N°	2018-2-10-000264	

Montevideo, 23 de abril de 2019

VISTO: La denuncia presentada contra la Facultad de Psicología de la Universidad de la República Oriental del Uruguay, por publicación de listado en Plataforma EVA sin consentimiento.

RESULTANDO:

1. Que la denunciante manifiesta ser alumna de la Facultad de Psicología y que una de sus docentes subió a la Plataforma EVA un listado con datos de sus alumnos, incluyéndola sin su consentimiento.
2. Que se dio vista a la Facultad de Psicología, la que evacuó argumentando que no existía vulneración a las normas de protección de datos personales, considerando que la comunicación de datos se encontraba amparada en las normas vigentes en la materia.

CONSIDERANDO:

1. Que la relación existente entre la institución y el alumno es consensuada, de consentimiento libre, previo y expreso, pero esa relación no se basa solo en la normativa que impera en la institución, sino en todas aquellas normas aplicables a nivel nacional como es el caso de la Ley Nº 18.331, de 11 de agosto de 2008.
2. Que en el caso es aplicable en concreto lo dispuesto por los artículos 9º y 17º, que establecen el principio del previo consentimiento informado y sus excepciones, y la comunicación de datos respectivamente. Adicionalmente, corresponde considerar la aplicación del artículo 9º bis, que regula las fuentes públicas de información.
3. Que las calificaciones de cada materia tienen como destinatario los alumnos y son anotadas en su escolaridad, por lo que la difusión de sus notas a través de la plataforma EVA o de cualquier otro medio, resultan una comunicación de datos de carácter personal que requiere el consentimiento (art. 17 de la Ley).
4. Que en el caso de obrados no resulta aplicable ninguna excepción al consentimiento de las previstas en el artículo 9º. Por otra parte, la Plataforma EVA no se enmarca en ninguna de las fuentes públicas de información referidas en el artículo 9º bis de la Ley.
5. Que al no existir en nuestro país una norma que prevea la comunicación de estos datos -como sí sucede en otros países-, la comunicación en la forma denunciada en obrados no se ajusta a las normas en materia de protección de datos, y requerirá del previo consentimiento informado del titular del dato -el estudiante-.

ATENTO: A lo expuesto e informado,

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

RESUELVE:

1. Recomendar a la Facultad de Psicología de la Universidad de la República Oriental del Uruguay que se incluya en la Plataforma EVA una cláusula de consentimiento cada vez que el alumno ingrese por primera vez a su usuario, con el fin de consentir la publicación y comunicación de sus notas a terceros, y establecer mecanismos alternativos en caso de que se deniegue dicho consentimiento.
2. NOTIFÍQUESE, PUBLÍQUESE Y OPORTUNAMENTE ARCHÍVESE.

DR. FELIPE ROTONDO

URCDP

Resolución Nº 21/019, de 14 de mayo de 2019

Se autoriza la transferencia internacional de datos presentada por Centro Ceibal para el Apoyo a la Educación de la Niñez y la Adolescencia.

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

RESOLUCIÓN N°	21	2019
Expediente N°	2018-2-10-000541	

Montevideo, 14 de mayo de 2019

VISTO: La solicitud de autorización para la transferencia internacional de datos presentada por CENTRO CEIBAL PARA EL APOYO A LA EDUCACIÓN DE LA NIÑEZ Y LA ADOLESCENCIA.

RESULTANDO:

1. Que se solicita la autorización de transferencia internacional de los datos referidos en documento presentado por la peticionante.
2. Que analizada la documentación presentada y las aclaraciones pertinentes, se produjo informe indicando que se ajusta a 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).

CONSIDERANDO:

1. Que el artículo 23 de la Ley Nº 18.331, de 11 de agosto de 2008, establece que la Unidad Reguladora y de Control de Datos Personales podrá autorizar una o una serie de transferencias a terceros países que no garanticen un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. Establece asimismo que dichas garantías podrán derivarse de cláusulas contractuales apropiadas.
2. Que se analizó la documentación presentada, considerándose que ofrece las garantías requeridas por la norma.

ATENTO: A lo expuesto e informado, y lo previsto en el artículo 23 de la Ley N° 18.331

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

RESUELVE:

1. *Autorícese* la transferencia internacional de datos en los términos solicitados por CENTRO CEIBAL PARA EL APOYO A LA EDUCACIÓN DE LA NIÑEZ Y LA ADOLESCENCIA.
2. *Inscríbase* la autorización otorgada en el Registro que lleva adelante esta Unidad.
3. *Notifíquese, publíquese* y oportunamente *archívese*.

DR. FELIPE ROTONDO

URCDP

Resolución Nº 22/019, de 14 de mayo de 2019

Se resuelve sobre la denuncia presentada contra una empresa en relación con la comunicación de datos personales a terceros.

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

RESOLUCIÓN N°	22	2019
EXPEDIENTE N°	2018-2-10-0000249	

Montevideo, 14 de mayo de 2019

VISTO: La denuncia formulada por el señor Aparicio Grosse contra la empresa CASH S.A.

RESULTANDO:

1. Que la denuncia versa sobre la comunicación de sus datos personales a terceros sin su consentimiento.
2. Que expresa el denunciante que la empresa Cash SA brindó información a su esposa, relativa a deudas, trámites de refinanciación, fechas y retención de sueldo entre otros datos relativos a su persona, brindando aquella únicamente nombre del denunciante y cédula de identidad. Por su parte la empresa denunciada aporta las grabaciones de las llamadas efectuadas.
3. Que surge de los escritos presentados por Cash S.A. (Fs. 15, 29 y 38), y de las grabaciones aportadas, que la operadora, sin corroborar la identidad de su interlocutor (más allá de indicar que la cédula de identidad proporcionada correspondía a un hombre y no a una mujer), brinda información referente al señor Grosse (cuotas, refinanciación, cumplimiento del convenio entre otras informaciones).

CONSIDERANDO:

1. Que se verificó una comunicación de datos en los términos establecidos en los artículos 4° literal B y 17 de la Ley N° 18.331 de 11 de agosto de 2008, así como un incumplimiento del artículo 10 de esta, por cuanto no se han adoptado las medidas de seguridad o establecido procedimientos que garanticen la confidencialidad de la información tendientes a evitar la consulta no autorizada de esta.
2. Que en lo que tiene que ver con el principio de reserva y confidencialidad, precisamente el art. 7° de la Ley referida (Principio de Veracidad) establece que la recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones de la Ley.
3. Que específicamente en aplicación de los artículos 7° y 11 de la ley antes referida, aquellas personas físicas o jurídicas que obtuvieron legítimamente información proveniente de una base de datos, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros, lo que en el caso de marras claramente no ocurrió.
4. Que agrega el artículo 11, que las personas que, por su situación laboral u otra forma de relación con el responsable de la base, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público
5. Que en lo que tiene que ver con el previo consentimiento informado, la denunciada señala que el Sr. Grosse ha sido cliente de Cash SA por más de 20 años, hecho que no implica de modo alguno que haya prestado su consentimiento para que otras personas accedan a sus datos personales, verificándose un incumplimiento de lo preceptuado en los artículos precitados. En aplicación del artículo 12 de la ley referida, Cash S.A. es responsable por los incumplimientos señalados.

ATENTO: A lo expuesto e informado,

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

Personales

RESUELVE

1. Sancionar a Cash SA con multa de 6001 unidades indexadas por haber incumplido con las disposiciones de la Ley N° 18.331 de 11 de agosto de 2008, en particular los artículos 5°, 7°, 10, 11 y 12.
2. *Notifíquese, publíquese y oportunamente archívese.*

DR. FELIPE ROTONDO

Resolución Nº 25/019, de 28 de mayo de 2019

. Se resuelve una denuncia por publicación en Internet de certificados médicos de una trabajadora luego de culminada su relación laboral.

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

RESOLUCIÓN N°	25	2019
Expediente N°	2019-2-10-000008	

Montevideo, 28 de mayo de 2019

VISTO: La denuncia por publicación en Internet de certificados médicos de una trabajadora luego de culminada la relación laboral.

RESULTANDO:

1. Que la denunciante expresa que la relación laboral entablada con el denunciado se tornó insoportable, por lo que se consideró indirectamente despedida llevando el trámite a la vía judicial. Afirma que cuando el denunciado tomo conocimiento de tal circunstancia comenzó a recibir amenazas y mensajes de textos intimidatorios y en uno de ellos se indicaba que sus referencias personales fueron subidas al buscador Google.
2. Que ante los mensajes recibidos, la denunciante constató que se habían subido certificados médicos donde se la identificaba y donde surgían datos sensibles, por lo que mediante telegrama solicitó su supresión. Posteriormente recibió un telegrama donde se expresaba que las publicaciones se realizaban en base a la libertad de expresión, y la baja de los certificados sólo se realizó luego de una instancia de conciliación, suplantándose por un aviso general de que la persona no se desempeñaba más para la empresa.
3. Que se procedió a dar vista de la denuncia, la que fue evacuada por el denunciado indicando que en su sitio web sólo se encuentra publicada información de que la denunciante no se desempeña más allí y que esa comunicación de datos está permitida por el literal c) del artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008. Complementariamente agrega que *"En el mes de julio del año 2018 y tan sólo durante algunos días fueron publicados certificados médicos…*,"y señala que existe una campaña de desprestigio contra su persona y que la denunciante era persona de confianza.

CONSIDERANDO:

1. Que no corresponde a esta Unidad expresarse en relación con las diferencias laborales existentes, sino analizar la legalidad de las comunicaciones de datos personales realizadas en el marco de la Ley N° 18.331, puntualizando que se trata de dos publicaciones distintas: la primera donde se publicaron certificados médicos de la denunciante y el segundo donde se informa sobre las personas que se encuentran desvinculadas de la empresa, indicando solamente sus nombres.
2. Que para realizar comunicación de datos personales es necesario contar con el previo consentimiento del titular así como con la existencia de interés legítimo del emisor y del destinatario de conformidad con lo dispuesto en el artículo 17 de la Ley N° 18.331. Además, en el caso de datos sensibles como los de salud, resulta de aplicación el artículo 18 de la Ley N° 18.331, de 11 de agosto de 2008, por el cual es necesario recabar el consentimiento expreso y escrito de sus titulares para todo tratamiento.
3. Que en lo que respecta a la segunda publicación no existe vulneración de la ley, en tanto existe un interés de la empresa en informar que determinadas personas no se encuentran más vinculadas a ésta, para lo que no se requiere su consentimiento.
4. Que con respecto a la primera publicación, donde se comunicaron datos de salud de la denunciante, no surge probada la existencia de ninguno de los elementos requeridos por el citado artículo 17 de la Ley, no siendo de aplicación al caso concreto ninguna de las excepciones allí dispuestas, incumpliéndose además con el artículo 18.
5. Que la publicación de datos sensibles es reconocida por la parte demandada en su escrito, no siendo la brevedad temporal de la publicación éste un elemento suficiente para no considerar lesionados los datos personales de la denunciante. Surge además comprobado que la denunciante no consintió su publicación y solicitó su baja en más de una ocasión por lo que la conducta de la denunciada constituye una infracción de carácter grave a la protección de datos personales.

ATENTO: a lo expuesto

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

RESUELVE:

1. Sancionar a Daniel KLIMAN (CONTROL KILOS) con multa de doce mil una unidades indexadas por incumplimiento de la Ley.
2. NOTIFÍQUESE Y PUBLÍQUESE

DR. FELIPE ROTONDO

URCDP

Resolución Nº 27/019, de 28 de mayo de 2019

Se resuelve una denuncia en relación con la instalación de una cámara de videovigilancia en posible infracción a los requerimientos de protección de datos personales.

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

RESOLUCIÓN N°	27	2019
EXPEDIENTE N°	2018-2-10-000558	

Montevideo, 28 de mayo de 2019

VISTO: La denuncia presentada en relación con la instalación de una cámara de videovigilancia en presunta infracción a los requerimientos de protección de datos personales.

RESULTANDO:

1. Que con fecha 22 de octubre de 2018, se presentó la denunciante manifestando que existe una cámara que enfoca hacia la entrada de su residencia y que la denunciada no posee autorización por parte de la copropiedad para su instalación. Se dio vista a la denunciada, la que no presentó descargos.
2. Que en virtud de las actuaciones llevadas a cabo, se dio vista a la Administración del Edificio para que ratifique el contenido de la nota presentada por la denunciante, y aportara información sobre el propietario del padrón, lo que efectivizó oportunamente. Complementariamente, se solicitó información sobre el titular del padrón, la que resultó incompleta.
3. Que se acreditó la existencia de una cámara no inscripta en el Registro de la Unidad que apuntaba hacia a entrada del domicilio de la denunciante sin logos identificatorios y se dio vista a la denunciada, quien la evacuó luego del informe solicitando sanción, expresando que la empresa retiró la cámara de filmación colocada con fines de seguridad y que la empresa que la instaló no les informó de los requisitos legales existentes.

CONSIDERANDO:

1. Que el presente caso versa sobre la instalación de cámaras de videovigilancia en una propiedad horizontal, estando en presencia de datos personales de conformidad con la definición del artículo 4° literal d) de la Ley N° 18.331.
2. Que el Consejo Ejecutivo de la Unidad por Dictamen N° 10/010, de 16 de abril de 2010, definió la videovigilancia y estableció las condiciones de uso de los sistemas, los principios aplicables y el registro de base de datos personales. Indica además que en aplicación del principio de veracidad (artículo 7° de la Ley), los sistemas de videovigilancia son subsidiarios, y solamente pueden utilizarse cuando no existen otros medios menos lesivos de la intimidad de las personas.
3. Que en cuanto a la necesidad de contar con logos de videovigilancia, cabe indicar que su patrón fue aprobado por Resolución de este Consejo N° 989/010, de 30 de julio de 2010.
4. Que en la Guía de videovigilancia en edificios, complejos y cooperativas emitida por la URCDP, se indica que*"Las cámaras que se utilicen solo podrán enfocar los espacios comunes y que sean considerados de vigilancia necesaria. En el caso de los edificios, se consideran espacios comunes las escaleras, los ascensores, el hall de entrada, los pasillos y cualquier otro determinado por el reglamento de copropiedad, siempre teniendo presente que el número de cámaras no debe ser desproporcionado al área que se vigilará".*
5. Que en el presente caso, surge probada la existencia de una cámara instalada en el Edificio que apunta hacia la puerta de entrada del domicilio de la denunciante, carente de logos de videovigilancia, y no registrada en el Sistema de Registros de Bases de Datos Personales. Por otra parte, fue instalada sin autorización de la copropiedad y no se conoce el destino de las grabaciones realizadas, no siendo suficiente la expresión de disculpas vertidas en el escrito de descargos.
6. Que de conformidad con el artículo 4° literal k) de la Ley N° 18.331, de 11 de agosto de 2008, el responsable es la persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento. En ese sentido surge clara la responsabilidad de COSTA Y COSTA S.A.
7. Que cabe agregar que la conducta de la denunciada es tachable desde el punto de vista jurídico en la medida que cuando se le notificó de la denuncia tomó conocimiento de la situación pero no contestó la vista conferida y solamente cuando se lo intima bajo apercibimiento contesta la vista.
8. Que además la cámara fue instalada por una tercera empresa, la cual no informó de estos requisitos, por lo que se requerirá se informen los datos identificatorios de ésta a fin de que tome conocimiento de la normativa en la materia.

ATENTO: a lo expuesto,

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

RESUELVE:

1. Sancionar a COSTA Y COSTA S.A. con apercibimiento por incumplimiento a la ley de protección de datos personales.
2. Intimar a COSTA Y COSTA S.A. a que en un plazo de 30 días corridos informe los datos identificatorios de la empresa que instaló las cámaras objeto de estas actuaciones.
3. NOTIFÍQUESE Y PUBLÍQUESE

DR. FELIPE ROTONDO

URCDP

Resolución Nº 28/019, de 28 de mayo de 2019

Se resuelve una denuncia contra un banco de plaza por errónea calificación y no actualización de datos personales del denunciante.

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

RESOLUCIÓN N°	28	2019
Expediente N°	2018-2-10-0000485	

Montevideo, 28 de mayo de 2019

VISTO: La denuncia realizada por el Sr. AA contra el Banco Central del Uruguay (BCU) por errónea calificación y no actualización de sus datos personales.

RESULTANDO:

1. Que el denunciante indica que realizó una reclamación *"al BCU por ser errónea la calificación al 31/jul/2018 a la Central de Riesgos por parte del Banco Santander, Banco Itaú, Scotiabank y ANDA (8/ago./2018)",* habiéndose generado el error en lo informado por el BROU a junio/2018. Se le habría indicado además en BCU que debía iniciar la reclamación en cada uno de los bancos.
2. Que el 13 de agosto de 2018 informó al BCU que los bancos ya habían remitido la información, obteniendo como respuesta que habían recibido su denuncia, pese a lo cual habrían transcurrido 10 días hábiles sin que se efectuara la corrección.
3. Que aportó las respuestas recibidas de las empresas en la que se le indica que *"tardarían dos o tres meses por falta de personal"* en modificar la calificación errónea, lo que ocurrió el 20 de setiembre de 2018 (fs. 34).

CONSIDERANDO:

1. Que conforme al artículo 4° literal K) de la Ley N° 18.331, de 11 de agosto de 2008 (LPDP) *"Responsable de la base de datos o del tratamiento: persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento".* En este sentido, corresponde señalar que si bien el BCU "administra" la Central de Riesgos Crediticios (CRC), encuadra en la figura de responsable antes reseñada pues decide sobre la finalidad, contenido y uso del tratamiento.
2. Que como consecuencia de lo expresado en el Considerando anterior, no se comparte la interpretación realizada a fojas 49 por el BCU cuando expresa *"que su rol no se adapta al concepto de "responsable" de la base de datos, en tanto, la ley atribuye la responsabilidad sobre la veracidad y actualización de los datos únicamente a las entidades de intermediación financiera que los proporcionan".*
3. Que corresponde tener presente el artículo 1° de la Ley N° 18.812, de 23 de setiembre de 2011: *"la Central de Riesgos Crediticios que administra el Banco Central del Uruguay está regulada por la Ley N° 18.331, de 11 de agosto de 2008, con las modificaciones y precisiones establecidas en los artículos siguientes".*
4. Que la Ley N° 18.331 se aplica en especial respecto de los plazos relativos a la rectificación o actualización de la información una vez recibida la información corregida de parte de las empresas, la que conforme con la citada norma debe efectuarse en 5 días hábiles, sin prórroga de ningún tipo.
5. Que el artículo 1° de la Ley N° 18.812 establece que el BCU tiene la competencia exclusiva de instrumentar y poner en funcionamiento la base de datos de la CRC. La comunicación N° 021/2012 de 24 de enero de 2012, contiene las instrucciones de carácter general que deberán seguir las instituciones de intermediación financiera. En este sentido, es recomendable adoptar todas las medidas necesarias para que los procesos internos, una vez ocurrido un reclamo/denuncia que finalice con la constatación de un error, se proceda con la mayor celeridad posible, para dar cumplimiento a los plazos legales y evitar generar un daño al titular de los datos personales.
6. Que la falta de adopción de medidas tendientes a garantizar la seguridad y confidencialidad de los datos personales como en el caso, se constituye en una vulneración de los 4° literal K), 5°, 10, 12, 15 y 22 de la Ley N° 18.331, tomando en cuenta el carácter de responsable de la base de datos del BCU.
7. Que en lo que respecta a las restantes obligaciones en el marco del artículo 12 de la Ley N° 18.331, de 11 de agosto de 2008, en la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018, corresponde por el tipo de tratamiento, la realización de una evaluación de impacto en la protección de datos personales.

ATENTO: a lo expuesto

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

RESUELVE:

1. Hacer saber al Banco Central del Uruguay que deberá adoptar medidas concretas que agilicen los procesos internos tendientes a resguardar la protección de datos personales y dar cumplimiento a lo dispuesto en el artículo 12 de la Ley N° 18.331, de 11 de agosto de 2008, en la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018, realizando a tales efectos una evaluación de impacto en la protección de datos, dando cuenta a esta Unidad.
2. NOTIFÍQUESE Y PUBLÍQUESE

FELIPE ROTONDO

URCDP

Resolución Nº 29/019, de 28 de mayo de 2019

Se resuelve una denuncia por utilización sin consentimiento de la imagen del denunciante.

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

RESOLUCIÓN N°	29	2019
Expediente N°	2018-2-10-0000543	

Montevideo, 28 de mayo de 2019

VISTO: La denuncia realizada por el señor Bruno Mauricio Albornoz contra EASY TAXI S.A. (en adelante Easy Go).

RESULTANDO:

1. Que el denunciante manifiesta indica que tomo conocimiento de que su *"imagen estaba siendo utilizada por la empresa, sin mi conocimiento, permiso, ni autorización para promocionar sus servicios en las Redes Sociales a través de "Historias" que son generadas por la Sra. Agustina Padilla durante sus viajes*". Agrega que "*La Sra. Padilla tiene un acuerdo con dicha empresa, por el cual a cambio de generar las "Historias" obtiene viajes gratis*". Aporta captura de pantalla de una historia de Instagram (fs. 6).
2. Que de la denuncia presentada se procedió a dar vista a Easy Go, la que indica que no difundió ni utilizó de forma alguna, imágenes del denunciante, habiéndolo hecho en todo caso un tercero. Agrega que si algún tercero difundió las imágenes "*fue por su cuenta y riesgo y no en representación ni en cumplimiento de algún contrato mantenido con esta empresa*". Agregan que no poseen contratos o acuerdos que implique para su cumplimiento difusión de imágenes de conductores y desconocen la autenticidad de la captura de pantalla agregada por el denunciante.
3. Que se dio vista nuevamente al denunciante para que aportara las imágenes referidas con los recaudos necesarios, lo que no ocurrió, por lo que dicha prueba no es admisible (artículo 70 del Decreto 500/991). Asimismo manifestó que mantuvo reunión con la Sra. Adriana Vicuña Manager Operations de Easy Uruguay, la que le informó "en forma presencial, personal y directa" que la empresa tenía un contrato con la Sra. Padilla para la generación de las citadas "Historias".
4. Que atento a la discordancia entre los dichos de ambas partes, se convocó a audiencia de testigos a la Sra. Adriana Vicuña, informando la denunciada que la testigo fue dada de baja de la empresa y se encuentra fuera del país. Se dio vista además a la Sra. Agustina Padilla, la que manifestó la inexistencia de cualquier relación con la denunciada.

CONSIDERANDO:

1. Que no surge probado incumplimiento a la normativa de protección de datos personales, ni se ha acreditado en debida forma la utilización de imágenes que identifiquen o hagan identificable al denunciante, en los términos del artículo 4 literal D) de la Ley N° 18.331 de 11 de agosto de 2011 (LPDP).
2. Que tampoco resulta acreditado que la publicación referida haya sido realizada por la empresa Easy Taxi S.A. por si ni por interpuesta persona, en tanto no se ha comprobado una relación contractual con la Sra. Padilla. En mérito a ello, no se ha probado la existencia de una comunicación de datos sin el consentimiento del titular en los términos del artículo 17 de la LPDP

ATENTO: a lo expuesto

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

RESUELVE:

1. Archívense las presentes actuaciones por no constatarse en estas actuaciones incumplimiento a la normativa en protección de datos personales.
2. *NOTIFÍQUESE Y PUBLÍQUESE.*

DR. FELIPE ROTONDO

URCDP

Resolución Nº 31/019, de 2 de julio de 2019

Se resuelve una denuncia referida a la utilización de datos personales sin el previo consentimiento de su titular.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES		
RESOLUCIÓN N°	31	2019
EXPEDIENTE N°	2018-2-10-0000175	

Montevideo, 2 de julio de 2019

VISTO: La denuncia formulada por la señora AA contra Heckler Bar (FABETUR S.A.) por presunto incumplimiento de la Ley N° 18.331, de 11 de agosto de 2008.

RESULTANDO:

1. Que la denuncia versa sobre la utilización de los datos de la denunciante sin su previo consentimiento, expreso, previo e informado.
2. Que del escrito presentado por la denunciada surge que el número telefónico de la Sra. Saavedra fue obtenido por haber ésta efectuado una reserva o cancelación a uno de los otros dos bares administrados por la denunciada (“El Garibaldi” o “El Comedy”) o por haber efectuado pedidos de delivery.
3. Que expresa la denunciante que concurrió una única vez al bar “El Garibaldi”, en el cual no se le informó que sus datos serían incluidos en la base de datos de la empresa para la comunicación de la apertura de otros bares, o la finalidad para la cual serían utilizados, así como tampoco se le informó del resto de los extremos requeridos en el artículo 13 de la ley citada.

CONSIDERANDO:

1. Que Habiendo solicitado la Sra. Saavedra la remoción de su número telefónico de la base de datos, resultan de aplicación los artículos 15 y 21 de la citada ley, por los cuales debió eliminarse el número telefónico.
2. Que conforme al artículo 6° de la Ley citada la formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establece la ley, extremo que no ha sido cumplido por la denunciada.

ATENTO: A lo expuesto e informado,

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

Personales

RESUELVE:

1. Impónese a FABETUR S.A. sanción de apercibimiento por haber incumplido con las disposiciones de la Ley N° 18.331 de 11 de agosto de 2008.
2. Intímese a FABETUR S.A. la inscripción de las bases de datos que posea ante esta Unidad en un plazo de 30 días hábiles.
3. *Notifíquese y publíquese.*

DR. FELIPE ROTONDO

URCDP

Resolución Nº 33/019, de 2 de julio de 2019

Se resuelve una denuncia por presunto incumplimiento del derecho de supresión.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES		
RESOLUCIÓN N°	33	2019
EXPEDIENTE N°	2018-2-10-0000532	

Montevideo, 2 de julio de 2019

VISTO: La denuncia formulada por el señor AA contra Instituto INFA (CHICAHUAC SRL), por presunto incumplimiento del derecho de supresión.

RESULTANDO:

1. Que la denuncia versa sobre el envío de mensajes al celular del Sr. Morales ofreciéndole becas, pese a haber solicitado al denunciante previamente que no se le enviaran más mensajes, acreditando el ejercicio del derecho de supresión.
2. Que CHICAHUAC SRL expresa, que *"por un error involuntario (…) el Sr. Morales recibió mensajes del centro educativo invitándolo a cursar materias que brindamos"* y que han anulado los datos pertenecientes al denunciante de la base de datos.
3. Que el argumento relacionado con el padecimiento de un error involuntario no se considera suficiente como para relevar la responsabilidad por los actos de publicidad realizados. A ello debe agregase que no fue una sola vez que el denunciante ejerció el derecho de supresión, sino que fueron varias las solicitudes realizadas por el denunciante, las que no fueron atendidas por la denunciada.

CONSIDERANDO:

1. Que resulta de plena aplicación al caso los artículos 7°, 9°, 12, 15 y 21 de la Ley N° 18.331 de 11 de agosto de 2008 en cuanto ha utilizado los datos sin el consentimiento de su titular, no ha permitido el ejercicio pleno del derecho de supresión de sus datos personales al denunciante.
2. Que conforme al artículo 15 de la ley citada la empresa cuenta con un plazo de 5 días hábiles para hacer efectivo el derecho de supresión, lo cual no ocurrió en el caso.

ATENTO: A lo expuesto e informado,

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

Personales

RESUELVE

1. Impónese a CHICAHUAC SRL sanción de observación por haber incumplido con las disposiciones citadas de la Ley N° 18.331 de 11 de agosto de 2008.
2. *Notifíquese y publíquese.*

DR. FELIPE ROTONDO

URCDP

Resolución N° 48/019, de 22 de noviembre de 2019

Se resuelve una denuncia referida a la incorporación indebida del denunciante a un bureau de crédito por parte de la empresa denunciada.

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

Datos de la Resolución

RESOLUCIÓN N°	**48**	**2019**
Expediente N°	2017-2-10-0000475	

Montevideo, 22 de noviembre de 2019

VISTO: La denuncia presentada contra AM WIRELESS URUGUAY S.A. (en adelante CLARO)

RESULTANDO:

1. Que la denunciante indica que ha sido indebidamente ingresada a un bureau de crédito por parte de la empresa denunciada y que ha recibido llamadas solicitando regularice su situación financiera. Ante ello, expresa que se comunicó con la denunciada donde le informaron que ya registra adeudos, y adjunta prueba de sus dichos.
2. Que de la denuncia se procedió a dar vista a EQUIFAX URUGUAY S.A. y FIEICOMISO MERCURIUS. Al evacuar la vista, la primera indicó que se procedió a dar de baja el registro tal como se le informó oportunamente al titular e indican que por tanto no son parte de la relación de autos. FIDEICOMISO MERCURIUS por su parte expresó que posee un contrato con la demandada por la cual ésta le cede una cartera de clientes donde se encuentran los datos personales de la denunciante, indicando que es el cedente el encargado de proporcionar toda la información pertinente relacionada con la deuda cedida, por lo que desconocen su origen y han cesado las llamadas.
3. Que ante los descargos presentados, se procedió a dar vista a CLARO, quien presenta un recuento de los montos abonados durante la relación contractual y expresan que la línea fue adjudicada telefónicamente en forma prepaga, migrándose a un abono mensual de la misma forma, y se procedió a transferir la deuda a un fideicomiso. El 21 de noviembre quedó anulado el contrato y se liberó de la deuda a la denunciante.
4. Que con fecha 20 de diciembre de 2017, se realizó el informe jurídico N° 366 por el cual se entiende que la denunciante ha vulnerado los principios de veracidad y previo consentimiento informado de la Ley N° 18.331, por lo que se recomendó oportunamente la imposición de sanciones.
5. Que del presente informe se procedió a dar vista a la denunciada, quien expresó que los datos personales tratados de la denunciante fueron los nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento, y que por tanto no requieren de consentimiento de acuerdo con lo dispuesto en el artículo 9 literal c) de la Ley N° 18.331, de 11 de agosto de 2008. También indica que la supresión de la información y la extinción de lo adeudado eliminan el agravio causado a la persona.

CONSIDERANDO:

- I. Que el presente caso versa sobre la adjudicación de una línea telefónica a una persona sin demostrar las medidas que adoptaron a los efectos de verificar su identidad. Además, se realizó una migración del tipo de contrato sin verificar la identidad del titular.
- II. Que resulta de aplicación la Ley N° 18.331, de 11 de agosto de 2008.
- III. Que existe una vulneración al principio de veracidad regulado en el artículo 7° de la citada norma en tanto que los datos que se recolectan deben ser veraces y que cuando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento deberá suprimirlos, sustituirlos o completarlos según el caso, En el caso no existe prueba de que se haya verificado que la persona a la que se adjudicó la línea era la denunciante, mediante mecanismos de identificación.
- IV. Que asimismo, resulta vulnerado el principio de previo consentimiento informado regulado en el artículo 9 de la misma norma, atento a la comunicación realizada a FIDEICOMISO MERCURIUS y EQUIFAX URUGUAY S.A.

ATENTO: a lo expuesto,

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

RESUELVE:

1. Sancionar a AM WIRELESS URUGUAY S.A. con 3001 UI (tres mil una Unidades Indexadas) por vulneración de los

principios de veracidad y previo consentimiento informado.

2. NOTIFÍQUESE Y PUBLÍQUESE

MAG. FEDERICO MONTEVERDE

URCDP

Resolución Nº 36/019, de 13 de agosto de 2019

Se resuelve una denuncia referida a la utilización de datos diferentes a los que se habían proporcionado.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES		
RESOLUCIÓN N°	36	2019
EXPEDIENTE N°	2018-2-10-0000772	

Montevideo, 13 de agosto de 2019

VISTO: La denuncia presentada por el Sr. AA contra SCOTIABANK URUGUAY S.A. y HENDERSON & CIA S.A. por utilización de datos sin consentimiento.

RESULTANDO:

1. Que el denunciante solicitó una tarjeta de débito a través de Tienda Inglesa a SCOTIABANK URUGUAY S.A., la que le llegó en tiempo pero con un domicilio diferente al que él había declarado. Realizó una solicitud de acceso a los datos que el banco tiene de su persona, por no recordar si realmente le había proporcionado el dato de ese domicilio y cumplido el plazo legal, el banco no contestó su pedido.
2. Que otorgada vista, SCOTIABANK URUGUAY S.A. manifiesta que el domicilio se encontraba en su base de datos desde 2007, y que fue facilitado por la cónyuge del denunciante en ese momento. Indica que el sistema toma ese dato para ser presentado al cliente, así este puede modificarlo o no si corresponde.
3. Que no fue cumplido por el banco en tiempo y forma el plazo establecido en el art. 14 de la Ley N° 18.331, ya que existió una demora interna del procedimiento de envío del correo electrónico al denunciante.
4. Que HENDERSON & CIA S.A. cumplió con lo solicitado por el denunciante enviando los datos proporcionados por el éste al banco.

CONSIDERANDO:

1. Que surge de estas actuaciones que SCOTIABANK URUGUAY S.A. no cumplió en tiempo y forma con el plazo establecido en el art. 14 de la Ley N° 18.331.
2. Que en lo referente a HENDERSON & CIA S.A., ésta cumplió con lo solicitado por el denunciante, enviando los datos proporcionados al banco, por lo que se entiende pertinente archivar estos obrados a su respecto.

ATENTO: A lo expuesto e informado,

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

Personales

RESUELVE:

1. *Apercibir* a SCOTIABANK URUGUAY S.A. por incumplimiento de la Ley N° 18.331, de 11 de agosto de 2008.
2. Archivar estas actuaciones con respecto a HENDERSON & CIA S.A.
3. Notifíquese, publíquese y oportunamente archívese.

MAG. FEDERICO MONTEVERDE

URCDP

Resolución Nº 37/019, de 13 de agosto de 2019

Se resuelve una denuncia referida a la comunicación de datos personales sin consentimiento.

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

RESOLUCIÓN N°	37	2019
EXPEDIENTE N°	2018-2-10-0000349	

Montevideo, 13 de agosto de 2019

VISTO: La denuncia formulada por el señor AA contra Escuela Brother (Mauricio Pablo Suarez Rassinetti) por comunicación de datos personales sin consentimiento.

RESULTANDO:

1. Que la denuncia planteada en estos obrados versa sobre la recepción de un correo electrónico invitando a completar un formulario de un Plan de Marketing de la Escuela, el cual se envió *"en forma masiva y con todas las direcciones visibles para todos"*.
2. Que surge del escrito presentado por la denunciada que con fecha 29 de mayo de 2018 dos estudiantes de la Escuela Técnica Superior de Administración y Servicios de la Universidad del Trabajo del Uruguay, *"fueron autorizadas a acceder a información de Brother únicamente con fines EDUCATIVOS y a los solos efectos de aprendizaje (…)*". Indica además que *"las estudiantes no son alumnas de la ESCUELA BROTHER y no tienen relación alguna con la institución"*.
3. Que Escuela Brother expresa que *"no solicitó el consentimiento informado porque el caso encuadraba como una excepción a los artículos 8 y 9 (…)"*.
4. Que agrega la denunciada que a los efectos de dar cumplimiento a los artículos 10, 11 y 12 de la Ley N° 18.331 de 11 de agosto de 2008, suscribieron con las estudiantes un acuerdo de confidencialidad "*en el cual las estudiantes se obligaron a no difundir información*". Aportan copia del acuerdo (fs. 30) e indican que *"las estudiantes fueron quienes difundieron la información y enviaron el mail, incumpliendo el acuerdo de confidencialidad suscrito y violando la Ley 18.331(…)"*

CONSIDERANDO:

1. Que el correo electrónico que recibió el denunciante identificaba a la Escuela Brother, único responsable desde el punto de vista de la protección de datos por aplicación del artículo 12. En este sentido, se verifica una vulneración del principio de finalidad (art. 8°) pues los datos objeto de tratamiento *"no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención"*.
2. Que Escuela Brother incumplió además el artículo 17 por efectuarse una comunicación sin el consentimiento del titular del dato ni encuadra dentro de las excepciones previstas en los literales A, B y C del mismo artículo. No resulta suficiente para deslindar la responsabilidad de la denunciada, el acuerdo presentado.
3. Que con rrespecto a la excepción prevista en el artículo 9° literal C), es de interpretación estricta, por lo que el consentimiento no está exceptuado para otros datos que no se encuentren en la enumeración taxativa.
4. Que no surge registro de base de datos por la denunciada, por lo que existe contravención de lo establecido en el artículo 6°.
5. Que la conducta de las señoras María Fernanda Gómez y Valentina Andrea Clavero encuadra en el incumplimiento del artículo 17 de la citada Ley, habiendo divulgado y comunicado los correos electrónicos sin el consentimiento del titular del dato, al haber enviado los correos electrónicos con todas las direcciones de correo electrónico a la vista.

ATENTO: A lo expuesto e informado,

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

Personales

RESUELVE:

1. *Apercibir* a Escuela Brother (Mauricio Pablo Suarez Rassinetti) por haber incumplido con las disposiciones de la Ley N° 18.331 de 11 de agosto de 2008.
2. *Apercibir* a María Fernanda Gómez y Valentina Andrea Clavero por haber incumplido el artículo 17 de la Ley citada.
3. *Intimar* a Escuela Brother (Mauricio Pablo Suarez Rassinetti) la inscripción de las bases de datos que sea titular en un plazo de 30 días hábiles.
4. *Notifíquese y publíquese.*

MAG. FEDERICO MONTEVERDE

URCDP

Resolución Nº 43/019, de 24 de setiembre de 2019

Se resuelve una denuncia referida al presunto incumplimiento del derecho de supresión.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES		
RESOLUCIÓN N°	43	2019
EXPEDIENTE N°	2018-2-10-0000500	

Montevideo, 24 de setiembre de 2019

VISTO: La denuncia formulada contra OVATSOL S.A., por presunto incumplimiento de la Ley N° 18.331 de 11 de agosto de 2008 en cuanto al derecho de supresión.

RESULTANDO:

1. Que la denuncia versa sobre el incumplimiento en la eliminación de los datos del denunciante, quien habría recibido confirmación excedido el plazo legal, y posteriormente recibió correo electrónico con publicidad de la empresa.
2. Que la empresa indica que se eliminó de la base de datos la información del denunciante, pero por “error” se omitió su eliminación de la lista de distribución de correos electrónicos de “MailChimp”.

CONSIDERANDO:

1. Que resultan de plena aplicación al caso los artículos 9° y 10 de la Ley citada (principios de previo consentimiento informado y de seguridad de los datos), por cuanto el responsable no ha adoptado las medidas necesarias que garanticen la seguridad y confidencialidad.
2. Que debe considerarse además lo establecido en los artículos 15 y 21 de la Ley referida, en cuanto al derecho de supresión de los datos relativos a bases de datos con fines de publicidad. En ese sentido, la denunciada incumplió los artículos considerados, en tanto ha utilizado los datos sin el consentimiento de su titular y no ha permitido el ejercicio pleno del derecho de supresión de sus datos personales al denunciante.

ATENTO: A lo expuesto e informado,

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

Personales

RESUELVE

1. Sancionar a Ovatsol SA con multa de 3001 UI (tres mil una unidades indexadas) por haber incumplido con las disposiciones de la Ley N° 18.331 de 11 de agosto de 2008, en particular los artículos 9°, 10, 15, y 21.
2. *Notifíquese y publíquese.*

MAG. FEDERICO MONTEVERDE

URCDP

Resolución Nº 44/019, de 24 de setiembre de 2019

Se resuelve una denuncia referida al incumplimiento del derecho de supresión.

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES		
RESOLUCIÓN N°	44	2019
EXPEDIENTE N°	2019-2-10-0000081	

Montevideo, 24 de setiembre de 2019

VISTO: La denuncia presentada contra ADT URUGUAY S.A. (en adelante ADT Uruguay) por no dar cumplimiento al ejercicio del derecho de supresión.

RESULTANDO:

1. Que el denunciante habría presentado ante ADT Uruguay una solicitud de derecho de supresión ante varias llamadas recibidas sin su consentimiento, rehusándose la denunciada a sellar o firmar una copia como acuse de recibo.
2. Que se le dio vista al denunciado de estos obrados quien manifiesta que no ha realizado estas llamadas en forma insistente y que los datos del denunciante fueron suprimidos de su base de datos.

CONSIDERANDO:

1. Que corresponde considerar la aplicación de los artículos 9° y 15 de la Ley N° 18.331, de 11 de agosto de 2008, que refieren respectivamente al principio de previo consentimiento informado –y sus excepciones- para el tratamiento de los datos y al ejercicio del derecho de supresión por parte de los titulares de éstos.
2. Que surge de obrados que no fue cumplido por el denunciado en tiempo y forma el plazo establecido en el artículo 15, en tanto la supresión se realizó luego de la notificación realizada por esta Unidad.

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

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

Personales

RESUELVE:

1. Sancionar a ADT Uruguay con observación por incumplir con los plazos legales para el ejercicio del derecho de supresión (Artículo 15 de la Ley N° 18.331, de 11 de agosto de 2008).
2. Notifíquese, publíquese y oportunamente archívese.

MAG. FEDERICO MONTEVERDE

URCDP

Resolución Nº 45/019, de 24 de setiembre de 2019

Se resuelve un oficio respecto al tratamiento de datos personales en dos organismos del Estado.

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

Resolución N°	45	2019
Expediente N°	2019-2-10-0000180	

Montevideo, 17 de setiembre de 2019

VISTO: El análisis de oficio respecto al tratamiento de datos de la Corte Electoral y la Dirección Nacional de Identificación Civil.

RESULTANDO:

1. Que en obrados se recopilaron varias denuncias vinculadas a la publicación en internet de un listado con información de electores uruguayos (nombres, apellidos y número de credencial cívica) y otro listado con datos de todas las cédulas de identidad del país, asociado a los nombres y apellidos de sus titulares.
2. Que se realizaron constataciones notariales de la página web mencionada en las denuncias, comprobándose la veracidad de los dichos de los denunciantes con respecto a la existencia de los listados y su contenido.
3. Que surge de la página web consultada que los datos habrían sido obtenidos de distintas páginas de entidades públicas –señalando además que la información de las cédulas fue obtenida de "diversos sitios web gubernamentales" y la de credenciales cívicas a través de una solicitud de acceso a la Corte Electoral-. El editor de la página señala que se habría consultado a esta Unidad, dónde se le habría indicado que la información de la Dirección Nacional de Identificación Civil es pública, y afirma además que la finalidad de la publicación es ubicar a personas con parentesco.
4. Que, con respecto a lo señalado en el considerando anterior, de los correos electrónicos que surgen de obrados resulta claramente la postura de la Unidad en el sentido de que la información provista por la Dirección Nacional de Identificación Civil no es pública (fs. 16).

CONSIDERANDO:

- I. Que nos encontramos ante bases de datos publicadas en forma libre en internet, por lo que resulta de aplicación lo establecido en el artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008.
- II. Que el artículo 17 precitado remite al artículo 9° de la misma ley, que respecto a las excepciones que habilitan el tratamiento de la información menciona las fuentes públicas (consagradas en forma taxativa en el artículo 9° bis de la Ley). Además, requiere en forma acumulativa la existencia de un interés del emisor y del destinatario de la información. En este caso la información de la Dirección Nacional de Identificación Civil y la Corte Electoral no se encuentra en ninguna de las excepciones previstas en el artículo, y no se aprecia además la existencia de un interés en el sentido en él señalado.
- III. Que, por otra parte, el hecho de que el artículo 9° literal C autorice el tratamiento de información en listados con nombres y apellidos y documento de identidad, entre otros, no lo justifica si éste no se realiza además al amparo de los restantes principios previstos en la Ley, y en el caso de la comunicación de datos, resulta necesario el cumplimiento de la acreditación del interés, lo que no se observa en obrados.
- IV. Que la finalidad de los datos contenidos en las bases de datos de la Corte Electoral y la Dirección Nacional de Identificación Civil se encuentra dada por una serie de normas (entre ellas el aartículo 21 del decreto-Ley N° 14.762 de 13 de febrero de 1979, y su tratamiento autorizado en especial por el artículo 151 de la Ley N° 16.736, de 5 de enero de 1996, y 81 de la Ley N° 16.462, de 11 de enero de 1994; la Ley N° 7.812 de 16 de enero de 1925, en la redacción dada por las Leyes N° 17.113, de 9 de junio de 1999 y 17.239, de 2 de mayo de 2000), la que no es compatible con la de las bases objeto de este análisis, por lo que se vulnera además lo establecido en el artículo 8° de la Ley N° 18.331.
- V. Que, por otra parte, las bases objeto de análisis resultan ilícitas, por no encontrarse inscriptas en el Registro que lleva adelante esta Unidad (artículo 6°), viciando de ilicitud todo el tratamiento realizado.

ATENTO: a lo expuesto e informado,

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

RESUELVE:

1. Intimar a los editores de la página web identificada en obrados a que retiren en forma inmediata el acceso a las bases de datos referidas en este expediente.
2. Dar vista de estas actuaciones a los editores de la mencionada página web y al señor AA, a efectos de que presenten los descargos que estimen pertinentes.
3. NOTIFÍQUESE Y PUBLÍQUESE

MAG. FEDERICO MONTEVERDE

URCDP

Resolución Nº 46/019, de 1 de octubre de 2019

Se resuelve una denuncia referida a la presunta falta de respuesta ante el ejercicio del derecho de acceso.

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

RESOLUCIÓN N°	46	2019
Expediente N°	2019-2-10-0000140	

Montevideo, 30 de setiembre de 2019

VISTO: La denuncia presentada contra la Dirección Nacional de Identificación Civil (en adelante DNIC) sobre la presunta falta de respuesta ante el ejercicio de derecho de acceso.

RESULTANDO:

1. Que el denunciante indica que presentó una solicitud de acceso a la información que existiera sobre su persona ante el Departamento de Gestión Documental de la DNIC, sobre la que no recibió respuesta y que le expresaron que se contactarían con él.
2. Que con fecha 30 de abril del corriente año, se procedió a dar vista de la denuncia a la DNIC, y que ante la no evacuación de vista, se la volvió a notificar.
3. Que con fecha 2 de julio de 2019, se realizó el Informe Jurídico N° 140, que analizando los plazos del ejercicio del derecho, indica que puede existir una posible conducta pasible de sanción por lo que se solicitó dar vista de acuerdo con lo dispuesto en el Decreto N° 500/991.
4. Que con fecha 25 de julio del corriente año, se agregó documentación proveniente de la DNIC de la que surge que con la solicitud del denunciante se conformó un expediente, con múltiples actuaciones.

CONSIDERANDO:

- I. Que el ejercicio del derecho de acceso se encuentra reconocido en el artículo 14 de la Ley N° 18.331, de 11 de agosto de 2008**,** el que debe ser habilitado dentro de los cinco días hábiles de la solicitud realizada por el titular de los datos.
- II. Que la Unidad, mediante Resolución N° 750/010, de 18 de junio de 2010, indicó que cuando una persona ejerza el derecho de acceso, el responsable de la base de datos sólo podrá exigir como requisito de la solicitud, la identificación del titular de los datos, cuestión cumplida por el denunciante.
- III. Que respecto a las actuaciones remitidas por el Ministerio del Interior cabe indicar que se procedió a efectivizar el ejercicio del derecho de acceso del titular de los datos, entregándole la información solicitada, pero fuera del plazo legalmente establecido.

ATENTO: a lo expuesto e informado.

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

RESUELVE:

1. Indicar a la Dirección Nacional de Identificación Civil que deberá ajustar sus procedimientos a fin de cumplir con las normas en materia de protección de datos personales, dando cuenta a esta Unidad
2. NOTIFÍQUESE Y PUBLÍQUESE

MAG. FEDERICO MONTEVERDE

URCDP