Introducción a la Protección de Datos Personales

Módulo 3

URCDP

Versión: 1

Año: 2024

1. Regímenes especiales de tratamiento de datos

a. Datos sensibles

Datos sensibles son todos aquellos datos personales que revelen el origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o la vida sexual de las personas. [1]

La Ley N° 18.331 indica que para el tratamiento de este tipo de datos se requiere el consentimiento expreso y escrito de los titulares de datos. Además, se prevé que solamente las instituciones que traten este tipo de datos pueden generar bases de datos con ese contenido.

b. Datos de salud:

Dentro del elenco de datos sensibles se encuentran los datos de salud, los que merecen una referencia particular. Se consideran datos de salud las informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona. Entre otros, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad o a su información genética[2].

Estos datos pueden recabarse por parte de los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud, los datos relativos a la salud física o mental de los pacientes que acudan a ellos o que hubieran estado bajo su atención profesional, respetando los principios del secreto profesional, la normativa específica y lo establecido en la Ley Nº 18.331.

c. Datos relacionados con el ámbito laboral:

En el ámbito laboral, el uso y tratamiento de los datos personales está limitado al contrato de trabajo y en mérito a éste es que se debe recabar la información necesaria para cumplir la función. Las normas en la materia deben

[1] Otras normas han ampliado el elenco de datos sensibles, tal como la Ley N° 19.172, de 20 de diciembre de 2013 que establece que los datos de identidad de los titulares de los actos registrados en el Instituto de Regulación y Control del Cannabis son datos sensibles (art. 28), y la Ley N° 19.869, de 2 de abril de 2020 que hizo la propio con respecto a todos los datos tratados en telemedicina (art. 8).
[2] Conforme el artículo 4° literal D del Decreto N° 414/009, de 31 de agosto de 2009.

complementarse con las normas laborales vinculadas a los sectores específicos de actividad y a las normas en materia de prevención de accidentes de trabajo, y de seguridad y salubridad laboral.

Corresponde señalar, además, que en lo que refiere a la documentación para la protección y control del trabajo establecida en la reglamentación respectiva, ésta se considera adecuada a los términos de la Ley N° 18.331, de conformidad con lo establecido en el artículo 84 de la Ley N° 19.355, de 19 de diciembre de 2015, en la redacción dada por el artículo 91 de la Ley N° 19.438, de 14 de octubre de 2016.

d. Datos de telecomunicaciones:

Las telecomunicaciones en todas sus variedades (por hilos, por aire, redes, telefonía, fax, mensajes de texto, televisión por cable y satelital, etc.) son merecedoras de especial atención, a los efectos de la protección de los datos personales.

Según la Ley, los operadores que exploten redes públicas y los que prestan servicios de comunicaciones electrónicas disponibles al público deben garantizar la protección de los datos personales conforme a la Ley. .

En ese sentido, se prevé la adopción de medidas particulares para presentar la seguridad en la explotación de su red o en la prestación de su servicio, e incluso se determina la obligación de informar a los abonados la existencia de riesgos de violaciones de seguridad a la red pública de comunicaciones electrónicas y las medidas a adoptarse.

Lo antedicho, sin perjuicio de las notificaciones que correspondan en caso de efectivas vulneraciones en mérito a lo establecido en el artículo 38 de la Ley N° 18.331.

e. Datos de Publicidad:

En el ámbito de la 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 titulares u obtenidos con su consentimiento.

En estos casos, el titular podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos, así como ejercer el derecho de acceso sin cargo alguno.

f. Datos de la actividad comercial o crediticia:

El tratamiento de datos destinado a informar sobre la solvencia patrimonial o crediticia está autorizado, 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.

Los datos deben ser obtenidos de fuentes de acceso público, o procedentes de informaciones facilitadas por el acreedor o en los casos previstos en la Ley.

Los datos personales relativos a obligaciones de carácter comercial de personas físicas sólo podrán estar registrados por un plazo de cinco años contados desde su incorporación.

En caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original.

Los responsables de las bases de datos se limitarán a realizar el tratamiento objetivo de la información registrada tal cual ésta le fuera suministrada, debiendo abstenerse de efectuar valoraciones subjetivas sobre ésta.

Cuando se haga efectiva la cancelación de cualquier obligación incumplida registrada en una base de datos, la persona acreedora deberá, en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo al responsable de la base de datos o tratamiento correspondiente. Una vez recibida la comunicación por el responsable de la base de datos o tratamiento, éste dispondrá de un plazo

máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación.

Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción, dejando expresa constancia de que están canceladas o extinguidas.

g) Datos biométricos

Si bien estos datos ya había sido reconocidos por el Consejo Ejecutivo de la Unidad como merecedores de una protección especial, la Ley N° 19.924, de 18 de diciembre de 2020 incorporó a la legislación nacional el concepto de datos biométricos, como datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona tales como datos dactiloscópicos, reconocimiento de imagen o voz (artículo 4° literal Ñ de la Ley N° 18.331). Reiterando la opinión de la Unidad en la resolución N° 30/020, el nuevo artículo 18 bis de la Ley N° 18.331 incluyó a los datos biométricos en el capítulo destinado a datos especialmente protegidos e impuso la obligación de los responsables y encargados de realizar evaluaciones de impacto previas a su tratamiento

2. Transferencias internacionales:

Nuestra Ley prohíbe la transferencia de datos personales de cualquier tipo a países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia.

Existen ciertas excepciones cuando se trata de: cooperación judicial internacional, intercambio de datos de carácter médico, transferencias bancarias o bursátiles, acuerdos en el marco de tratados internacionales en los cuales el Uruguay sea parte, cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

También es posible realizar la transferencia internacional de datos cuando la parte interesada haya dado su consentimiento inequívocamente a la transferencia prevista; si es necesaria para la ejecución de un contrato entre la parte interesada y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición de la parte interesada; si es necesaria para la celebración o ejecución de un contrato celebrado o por celebrarse entre el responsable y un tercero, en interés de la persona interesada; si es 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; si es necesaria para la salvaguardia del interés vital de la persona interesada; o si tiene 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.

Sin perjuicio de lo anterior, la URCDP puede autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable 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.

Dichas garantías podrán derivar de cláusulas contractuales apropiadas. A estos efectos, el Consejo Ejecutivo emitió la resolución N° 41/021, de 8 de setiembre de 2021, en la que establece un contenido mínimo para dichas cláusulas

Corresponde indicar que, además, y en función de lo establecido por el artículo 6° del decreto N° 64/020, toda transferencia a un país u organización no adecuados deberá ser precedida de una evaluación de impacto en la protección de datos.

Ahora bien, las referidas previsiones son aplicables en el caso de países u organizaciones que no garantizan un nivel adecuado de protección, y en

consecuencia la transferencia debe basarse en alguna de ellas, y en su caso obtener la autorización previa de la Unidad.

No obstante, es posible efectuar una transferencia de datos sin acreditar estos extremos (aunque sí cumpliendo con todos los restantes principios y obligaciones de la Ley), cuando ésta se realiza a un país u organización considerada adecuada.

Por Resolución N° 23/021, de 8 de junio de 2021, se establece 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, 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[3].

Es importante destacar que la Unidad puede ampliar o reducir el elenco de países u organizaciones mencionados en la resolución anterior, por lo que es de suma importancia realizar una revisión en forma previa a cualquier transferencia por parte de responsables y encargados.

La resolución N° 63/023, de 21 de noviembre de 2023, incluye dentro del listado de la Resolución N° 23/021 de esta Unidad, a las transferencias internacionales realizadas a las entidades sujetas a la Ley de Protección de la Información de la República de Corea y a las transferencias a organizaciones incluidas en el “Listado del Marco de Privacidad de Datos” publicado por el Departamento de Comercio de los Estados Unidos de América[4].

Por su parte, la Resolución N° 70/023, de 5 de diciembre de 2023, expresa que los responsables y encargados de tratamiento que realicen transferencias

[3] https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021
[4] https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023

internacionales deberán comunicar a los titulares de los datos en las circunstancias previstas en el artículo 13 de la Ley 18.331, el destino de sus datos, el rol del importador, el plazo de transferencia, la base de legitimación y las operaciones de tratamiento realizadas por el importador. Además, indica que tanto los responsables como los encargados tienen un plazo de 6 meses para adaptar sus políticas de privacidad a lo indicado.

Esta misma Resolución refiere además a que la inscripción de la base de datos en el Sistema de Gestión de la URCDP es un requisito previo a toda operación de tratamiento, incluyendo las transferencias internacionales.

Por último, aclara que los responsables y encargados que realicen transferencias a organizaciones incluidas en el Marco de Privacidad UE- EEUU deben presentar ante esta Unidad cuando realizar la inscripción de la base de datos, o en forma previa a la transferencia, una declaración expresa en la que la respectiva organización importadora declare haber extendido la aplicación de las salvaguardas de dicho marco a los datos transferidos desde Uruguay. En caso de que no se formule dicha declaración la transferencia a las citadas organizaciones puede ser realizada en base a cláusulas contractuales presentadas por los responsables o encargados que sean autorizadas previamente por esta Unidad u otros fundamentos previstos legalmente[5].

3. Otros aspectos a tener en cuenta en el tratamiento de datos:

a. Criterios de disociación [6]

En materia de disociación la Unidad ha publicado la Guía de disociación la cual cuenta con diversos criterios de no identificación de aquellos datos personales

[5] https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-70023

[6] Conforme lo dispuesto por el Decreto N° 54/017, de 20 de febrero de 2017,reglamentario del artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015, en el que se establece que las Entidades Públicas, sujetos obligados por la Ley N° 18.381,de 17 de octubre de 2008, deberán proceder a la publicación de la información contenida en los artículos 5° de la Ley y 38 y 40 del Decreto N° 232/010, 2 de agosto de 2010, en formato de dato abierto, la URCDP, por Resolución Nº 68/017, de 26 de abril de 2017, aprobó el documento Criterios de Disociación de Datos Personales. Disponible en: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-criterios-disociacion-datos-personales

que se encuentran en la información que se deba publicar como dato abierto, como ser: seudonimización, disociación, anonimización entre otros.

Con estos criterios se pretende que toda persona que utilice estas técnicas incorpore los lineamientos dados en esta guía, para disminuir al mínimo la posibilidad de re-identificar al titular del dato que se maneje, teniendo en cuenta que esta es una actividad dinámica que varía por la constante aparición de nuevos mecanismos de re-identificación.

Si bien los criterios fueron generados con el objetivo de dar cumplimiento a las previsiones en materia de publicación de datos abiertos, su aplicación puede ser realizada por parte de cualquier responsable o encargado en el marco de cualquier operación de tratamiento de los datos.

b. Tratamiento de datos de menores

El tratamiento de datos de menores ha sido una constante preocupación por parte de la Unidad. Con criterio general se debe señalar que es necesario recabar el consentimiento de sus padres o tutores antes del tratamiento de los datos de menores.

Los responsables deben cuidar la utilización de este tipo de datos personales, debiendo considerar la finalidad y las medidas de seguridad como elementos esenciales previo a su análisis.

Recientemente, el decreto N° 64/020 (art. 6°) incluye dentro de las hipótesis en las cuales debe realizarse previamente una evaluación de impacto, el tratamiento de datos de menores. Ello por las consecuencias que puede acarrear una utilización incorrecta de este tipo de datos personales.

La Unidad ha trabajado en forma constante, generando contenidos y promoviendo actividades para la concientización de este derecho en menores de edad, de forma tal que tengan conocimiento de su existencia desde temprana edad.

c. Videovigilancia

Mediante la utilización de dispositivos de videovigilancia se pueden captar la imagen y la voz, los cuales son datos personales y por ende pasibles de protección según la normativa vigente.

La Unidad ha analizado esta temática desde sus comienzos, lo cual se refleja en el dictamen N° 10/010 de 16 de abril de 2010. En éste se expresa 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*". [7]

En este dictamen se indica que la captación o grabación de imágenes constituye información personal, por lo que resulta de aplicación la normativa vigente sobre protección de datos personales. Por ende, corresponde tener en cuenta los diversos aspectos que puede comprender la videovigilancia, esto es, qué puede ser videovigilado, de qué forma, qué principios son aplicables y si se deben registrar los resultados, entre otros.

Es de destacar que la videovigilancia tiene como principales finalidades la protección de las personas físicas, del derecho de propiedad, la tutela del orden público, la detección y prevención de delitos, así como otros intereses legítimos.

Esta norma establece además la necesidad de contar con logos de videovigilancia, cuyo patrón fue aprobado por resolución de la Unidad N° 989/010, de 30 de julio de 2010[8] [9].

La Resolución N° 58/021, de 21 de diciembre de 2021, resuelve el uso de cámaras en diversos ámbitos. En especial para aquellas cámaras utilizadas con finalidad personal o doméstica, con fines de seguridad pública, sobre aquellas que se utilicen en el ámbito de la actividad bancaria, en el ámbito laboral, en edificios y

[7] Puede consultarse el Dictamen en https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/dictamen-10010

[8] Puede consultarse la Resolución en https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-9892010

[9] Pueden descargarse los logos de https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/logo-videovigilancia-formato-horizontal-100mm-x-55mm

complejos habitacionales, por las Entidades Públicas, en vehículos y similares, en instituciones educativas primarias y secundarias y por drones[10].

[10] https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-58021