Memoria Anual 2021

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

Contenido

1. Actividades académicas de la Unidad de Protección de Datos Personales **3**

2. Principales temas del año **7**

3. Avances normativos **14**

4. Guías de protección de datos personales **19**

5. Jurisprudencia Nacional **20**

6. Difusión y capacitación de la Unidad **22**

7. Relacionamiento internacional **23**

8. La URCDP en cifras **24**

Actividades académicas de la Unidad de Protección de Datos Personales

Día internacional de la protección de datos.

El 28 de enero se celebró el Día Internacional de la Protección de Datos en todo el mundo, coincidiendo con el 40° aniversario del Convenio 108 del Consejo de Europa, primer tratado internacional vinculante en la materia.

Este Convenio fue actualizado por el Protocolo del año 2001 incluyendo normas respecto a flujos internacionales de datos y autoridades de protección de datos.

Uruguay, el 1° de agosto de 2013, se convirtió en el primer Estado no europeo en formar parte del Convenio y su Protocolo de 2021, que ya había sido internalizado por la Ley N° 19.030, de 27 de diciembre de 2012, y ha firmado el protocolo de modernización.

En 2018, su Protocolo Modificativo, conocido como Convenio 108+, se abrió a la firma con el fin de adaptar el Convenio a las nuevas tecnologías y fortalecer su mecanismo de seguimiento. Nuestro país suscribió el nuevo protocolo el 10 de octubre de 2018, fecha de apertura a firma.

Con la promulgación de la Ley N° 19.948, el 16 de abril de 2021, nuestro país se convirtió en el primer país de Latinoamérica en internalizar las disposiciones del convenio 108+.

En la actualidad, son miembros del Convenio original 55 Estados de distintas partes del mundo, 25 de los cuales han suscrito el protocolo de modernización.

Evento nacional de protección de datos personales: Uso y conservación de información personal.

El Evento anual de la Unidad constó de dos jornadas y versó sobre el tema *"Uso y conservación de la información personal"*. La apertura estuvo a cargo del Director Ejecutivo de Agesic, Hebert Paguas; el Miembro del Consejo Ejecutivo de la URCDP Felipe Rotondo; y el Coordinador de protección de datos, Gonzalo Sosa.

Hebert Paguas se refirió a la importancia de los datos personales en tres aspectos: la necesidad de contar con marcos normativos fuertes que garanticen su uso en aplicaciones tecnológicas, normas globales que potencien el accionar de la URCDP en el exterior y directivas claras a operadores que manejan datos en este contexto de pandemia.

Por su parte, Felipe Rotondo señaló la relevancia del buen uso y la conservación de información personal, teniendo en cuenta que no solo están en juego los aspectos jurídicos sino la dignidad de las personas, y se centró especialmente en el rol fundamental de los principios de la protección de datos.

Posteriormente, tuvo lugar la presentación "*Desafíos actuales para la Protección de Datos Personales*" de la Dra. Ana Brian Nougréres, relatora especial sobre la Privacidad de la Organización de las Naciones Unidas, quien expuso sobre las tensiones en el manejo de los archivos, el uso de la Inteligencia Artificial para la toma de decisiones, la video vigilancia a nivel masivo y la importancia de revisar las tendencias para su regulación. Por último, instó a inspirarse, crear e innovar sobre nuevas formas que permitan atender y resolver estas temáticas.

Finalmente, en el panel "*La conservación de la información personal más allá de la finalidad en los ámbitos público y privado*", María Alejandra Villar, responsable del Departamento de Gestión Documental de la Fiscalía General de la Nación e integrante del Consejo Ejecutivo de la UAIP, y Javier Wortman, escribano especialista en protección de datos personales y cocoordinador de la Comisión de Derecho Informático de la Asociación de Escribanos del Uruguay, analizaron las normas que regulan la conservación de la información en el ámbito público, especialmente la de conservación archivística y la conservación por parte de Escribanos Públicos en los registros notariales.

La jornada de cierre del evento se realizó el 1° de octubre y estuvo dividida en dos paneles. El primero, denominado

"*El uso intensivo de información personal en el ámbito público. Alcances y restricciones*", a cargo de María Laura Rodríguez, directora de Tecnología de Agesic; Federico Seguí, subdirector general del INE; y Carla Barboza, abogada asesora en relaciones gubernamentales en EQUIFAX, como moderadora del panel. Durante sus intervenciones abordaron la estrategia de datos a nivel nacional y las perspectivas para un uso intensivo de la información, con énfasis en los principios y las normas que regulan la protección de datos personales.

En el segundo panel "*El uso intensivo de información personal en el ámbito privado. Alcances y restricciones*" participaron Martín Pesce, abogado especialista en protección de datos y nuevas tecnologías de FERRERE, y co-chair de la International Association of Privacy Professionals; Leonardo Loureiro, gerente comercial de QUANAM y presidente de la Cuti; y Laura Nahabetián, directora del Instituto de Derecho Informático de la Facultad de Derecho, Udelar, como moderadora.

Finalizado el segundo panel, se realizó un cierre formal de la actividad.

Ciclo de Charlas de Café 2021

Primera charla de café: Aprobación del Convenio 108+

Con la participación del Jefe del Departamento de Sociedad de la Información del Consejo de Europa, el 27 de mayo se realizó la primera Charla de Café virtual del año sobre la aprobación del Convenio 108+, sus impactos y oportunidades para Uruguay.

El panel estuvo integrado por Patrick Penninckx, jefe del Departamento de Sociedad de la Información del Consejo de Europa; Marcelo Bauzá, miembro del Consejo Consultivo de URCDP por la academia; Felipe Rotondo, presidente del Consejo Ejecutivo de URCDP y Gonzalo Sosa, coordinador de datos personales, como moderador.

Penninckx describió el proceso de modernización del Convenio 108 y destacó el estrecho vínculo entre el Consejo de Europa y Uruguay, así como el rol del país y de la Unidad para el fortalecimiento del diálogo y la cooperación para el cumplimiento de la normativa, y garantizar el ejercicio del derecho de la protección de datos personales.

Asimismo, señaló los cambios sustantivos de la actualización del Convenio como las competencias de supervisión de las autoridades de control y el manejo de los datos biométricos. Además, mencionó otros aspectos que han sido abordados por el Consejo de Europa como la protección de datos en el contexto de la pandemia, el registro de vacunación, los pasaportes sanitarios y la protección de derechos y libertades fundamentales en cuestiones de salud pública, así como la necesidad de regulación del reconocimiento facial, la identidad digital y los desafíos que impone el actual contexto tecnológico, de rápida y constante evolución.

Por su parte, Marcelo Bauzá mencionó la importancia de adherir y ratificar el Convenio 108+, y reflexionó sobre el Convenio y varios de sus artículos. En tal sentido, hizo referencia a los antecedentes del país en la materia como la Ley N° 18.331 de Protección de Datos Personales y Habeas Data; y a nivel internacional la Declaración Universal de los Derechos Humanos de Naciones Unidas de 1948 y la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) de 1969. Con respecto al Convenio, puso énfasis en la importancia de afianzar la protección de datos como derecho humano y su foco en el ejercicio de este derecho en el actual contexto tecnológico.

Finalmente, Felipe Rotondo destacó la importancia de esta instancia y señaló la relevancia que tiene el análisis de los datos para la innovación y la competitividad; indicando que este desarrollo es válido sólo si se respetan los derechos humanos. En ese contexto, este Convenio se vuelve esencial para el control y la efectividad del cumplimiento de las normas en protección de datos personales y de derechos humanos en general en los Estados.

Segunda charla de café: Transferencias internacionales de datos

El 16 de setiembre se realizó la segunda Charla de Café del año en torno a los criterios de la URCDP y las cláusulas contractuales vinculantes en las Transferencias Internacionales de Datos.

Durante la actividad se analizó la evolución a nivel internacional del régimen de transferencias internacionales de

datos, así como la reciente resolución de la Unidad determinando los territorios adecuados para dichas transferencias, y la implementación de cláusulas contractuales vinculantes como mecanismo de garantía para los titulares de los datos.

Participó del panel el presidente de la Unidad, Felipe Rotondo, y el equipo técnico integrado por Gonzalo Sosa, Beatriz Rodríguez, Flavia Baladán y Lilyan Massarino.

Beatriz Rodríguez presentó los conceptos de transferencia de datos personales y su interpretación, la amplia regulación que tiene el país en la materia y las formas de tratamiento de los mismos a nivel nacional e internacional.

Flavia Baladán expuso el desarrollo del derecho de protección de datos personales y las diferentes perspectivas que existen de este derecho en Europa y Estados Unidos. Asimismo, realizó un análisis de las consecuencias internacionales de recientes fallos del Tribunal de Justicia de la Unión Europea y su impacto en las transferencias a los Estados Unidos, lo que motivó incluso los cambios que surgen de la reciente resolución de la Unidad en la materia.

Por su parte, Lilyan Massarino hizo énfasis en las cláusulas contractuales, con las que se tratan de defender los derechos de las personas en materia de protección de datos personales, que resultan de las resoluciones de la Unidad, y la necesidad de solicitar autorización a la Unidad cuando corresponde.

Otras actividades académicas de la Unidad

La Unidad participó del evento “Diálogos Latinoamericanos”

El día 9 de abril de 2021 se realizó un evento virtual en el marco de la actividad “Diálogos Latinoamericanos”, organizado por el Laboratorio de Políticas Públicas e Internet de Brasil (LAPIN), con el objetivo de analizar la gestión por cada organización de los incidentes de seguridad, los mecanismos de mitigación y coordinación.

El coordinador de la URCDP, Gonzalo Sosa, participó junto a la directora de la Agencia Nacional de Protección de Datos de Brasil, Nairane Rabelo, y el director de Protección de Datos Personales de la Agencia de Acceso a la Información Pública de Argentina, Eduardo Cimato.

En particular, Gonzalo Sosa destacó el proceso de modificación de la normativa uruguaya en la materia con la sanción de la Ley N° 19.670, de 15 de octubre de 2008, y su posterior reglamentación a través del decreto N° 64/020, de 17 de febrero de 2020. Realizó especial énfasis en la necesidad de contar con reglas claras para la comunicación de los incidentes, el rol de la responsabilidad proactiva, un adecuado análisis de riesgo centrado en las personas, y la colaboración del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) en dicho proceso.

URCDP en el I Foro Internacional de Privacidad y Protección de Datos

“*Desarrollos y Desafíos Regulatorios en la Sociedad Global*” fue la línea temática elegida para el Foro realizado de forma virtual entre el 17 y el 19 de mayo, en el que participó la Unidad.

Más de 20 autoridades de protección de datos de todo el mundo participaron de la primera edición de esta actividad organizada por el Observatorio Iberoamericano de Protección de Datos, el capítulo Madrid de la Asociación Internacional de Profesionales de Privacidad (IAPP), la Fundación PRIDAT y la Universidad de Nebrija.

El objetivo de la actividad fue presentar el estado de la regulación de los distintos países participantes y dar a conocer los retos que se plantean a nivel nacional y regional en lo que refiere a la protección de datos personales.

En este sentido, Gonzalo Sosa, coordinador de la Unidad, participó del panel organizado el día 18 de mayo sobre “*Retos y oportunidades de la protección de datos en América del Sur*”, junto a Eduardo Peduto Pardo, director del Centro de Protección de Datos de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires; Gloria de la Fuente, presidenta del Consejo para la Transparencia de Chile, y Lorena Naranjo, directora de la Dirección Nacional de Registro de Datos Públicos de Ecuador.

En el panel se comentó el estado de situación y desarrollo de las legislaciones nacionales y las perspectivas a futuro para la modernización de la normativa en el ámbito latinoamericano. Quienes expusieron coincidieron en la importancia de

desarrollar ámbitos regionales de cooperación que permitan a las autoridades de Latinoamérica asegurar el cumplimiento de la Ley, y la relevancia de participar en instrumentos internacionales, como el Convenio 108 del Consejo de Europa.

Seminario Internacional "Los retos de la protección de datos personales en la era digital"

URCDP participó de la 6ª sesión del Seminario Internacional organizado por el Sistema Nacional de Transparencia de los Estados Unidos Mexicanos. La sesión número seis del Seminario se realizó el 15 de julio de forma virtual y trabajó bajo la temática "Convenio 108 y Convenio 108 + y la protección de datos personales en México". La mesa fue moderada por Teresa Treviño, de la COTAI y contó con la participación de Liliana Campuzano, de la CEIAP; Gustavo Parra, de INFOEM; Josefina Román, de INAI; y Gonzalo Sosa, de la URCDP.

En la mesa se trataron los alcances, beneficios y desafíos que plantea el Convenio 108+ del Consejo de Europa para los países de América Latina. En su presentación, Gonzalo Sosa, desarrolló sobre la experiencia uruguaya en materia de protección de datos personales. Destacó la trayectoria que tiene el país en derechos humanos y su evolución, particularmente, con la consagración de la Ley N° 18.331 y el proceso de adhesión al Convenio 108 en 2013, y posteriormente, aprobar el protocolo de modernización del convenio 108+.

Asimismo, señaló la importancia de este convenio para Uruguay, por ser un instrumento universal abierto a otros países fuera de Europa, que establece bases comunes de cooperación, principios, estándares internacionales y un conjunto de autoridades independientes; y habilita entre las partes un flujo de datos seguro.

Evaluación de impacto en protección de datos

La Unidad presentó su experiencia en torno a la evaluación de impacto en protección de datos en el webinar "*Análisis de impacto en protección de datos personales y derechos humanos*", organizado por la Red Iberoamericana de protección de datos.

El Foro de la Sociedad Civil de la Red Iberoamericana de protección de datos, en contexto de emergencia sanitaria, inició un ciclo de webinars abiertos al público sobre temas relacionados con la privacidad y la protección de datos.

En el marco de este ciclo de actividades, el 9 de setiembre de 2021 se realizó el webinar "*Análisis de impacto en protección de datos personales y derechos humanos*", del que participaron representantes de instituciones de protección de datos de Brasil, Chile, Argentina, España y Uruguay.

Flavia Baladán, del equipo de la URCDP, expuso la experiencia de Uruguay en la creación de la "*Guía de evaluación de impacto en protección de datos*", un documento creado en conjunto con autoridades argentinas que busca ser una referencia obligada para las entidades de la región que realicen tratamiento de datos personales.

En su exposición, Baladán indicó cuándo es preciso realizar una evaluación de impacto, cuáles son los parámetros de los procedimientos, así como los espacios de evolución política y regulatoria en el contexto de cada país.

Por último, con el objetivo de contribuir a la agenda de derechos humanos, los participantes debatieron en torno a cómo el análisis de impacto en protección de datos, como instrumento legal, se relaciona con los derechos individuales y colectivos.

Foro virtual de IID y OEA

I Foro "*Los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales del CJI*", se realizó el 23 de setiembre en modalidad virtual. Participaron Dante Negro, director del Departamento de Derecho Internacional de OEA; Claudia Barrientos, representante de la OEA en Uruguay; Mariana Salazar Albornoz, miembro del CJI y relatora para el tema de protección de datos personales; Eduardo Bertoni, representante y coordinador de la Oficina Regional América del Sur de IIDH; Jaime Moreno-Valle, oficial jurídico principal del Departamento de Derecho Internacional de OEA y Felipe Rotondo, presidente del Consejo Ejecutivo de la URCDP.

Rotondo, en su exposición "*Los Estándares Iberoamericanos de Protección de Datos Personales y su Compatibilidad con los Principios Actualizados del CJI*" planteó la importancia de los estándares y principios de uso y protección de los datos personales en esta sociedad de la información, la cual debe estar centrada en las personas. Asimismo, señaló que las normas legales muchas veces quedan relegadas con el incesante cambio tecnológico, pero no así los principios, ya que son la esencia, explicitan valores superiores y contribuyen a dar coherencia y sirven de criterio interpretativo e integrativo de la ley.

Del mismo modo, se refirió a la situación de protección de datos en el país, en la que hay bases de datos excluidas de la ley, como por ejemplo bases de seguridad pública o de investigación de delitos, pero que no escapan de los principios capitales de la protección de datos.

Al finalizar, Rotondo destacó nuevamente el valor del CJI (Comité Jurídico Interamericano) y que los estándares desarrollados ya han influido en legislaciones en diversos países latinoamericanos, por lo que hay que seguir en un camino convergente que tanto la Red Iberoamericana de Protección de Datos, como la OEA, deben de proseguir.

43° Asamblea Global de Privacidad y XIX Encuentro de la Red Iberoamericana de Protección de Datos

Del 18 al 21 de octubre se desarrolló la 43ª. Asamblea Global de Privacidad (GPA), el foro mundial más importante en materia de privacidad y protección de datos del mundo. En este marco, tuvo lugar además el XIX Encuentro de la Red Iberoamericana de Protección de Datos (RIPD).

Los días 18 y 19 se realizaron varios paneles en los que las autoridades de protección de datos del mundo, la academia, el sector privado y organizaciones de la sociedad civil debatieron sobre el rol de la protección de datos frente a los avances tecnológicos y la inteligencia artificial.

Gonzalo Sosa, participó en calidad de expositor en el panel "*El Convenio 108+ y las perspectivas de un tratado global en inteligencia artificial*", moderado por Veronique Ciminá, representante del Supervisor Europeo de Protección de Datos, y con participación del Paul Breitbarth por el sector privado, Alessando Mantelero por la Academia y Jean-Phillipe Walter, por el Consejo de Europa.

El coordinador de URCDP, destacó los aspectos más relevantes del Convenio 108+, los motivos que llevaron a Uruguay a formar parte, y los beneficios que conlleva su adhesión.

La Asamblea Global se clausuró en la sesión cerrada, donde se pusieron a votación distintos documentos que se pondrán a disposición del público en el sitio web de la GPA , y se eligió como nuevo Presidente al Instituto Nacional de Transparencia, Acceso a la Información Pública y protección de Datos (INAI) de México.

En el marco de la 43ª. Asamblea, el 22 de octubre se desarrolló en formato virtual el XIX Encuentro anual de la Red Iberoamericana de Protección de Datos (RIPD), del que participaron todos los miembros y observadores de la Red, con Felipe Rotondo, miembro del Consejo Ejecutivo de la URCDP, como representante de la Unidad.

Durante la actividad, se trataron diversos temas vinculados a la estructura interna de la Red, se analizaron los avances en protección de datos en los países de la región, y se consideraron distintos documentos elaborados por la Red, para apoyar las iniciativas de las autoridades de protección de datos en Iberoamérica.

Principales temas del año

Sobre aspectos generales de la videovigilancia

La Unidad mediante Resolución N° 58/021, de 21 de diciembre de 2021, incorporó las condiciones para el uso de cámaras en diversos ámbitos, en función de los criterios ya adoptados en resoluciones anteriores, y el contenido de guías de buenas prácticas publicadas previamente.

Esta Resolución refiere a los aspectos a considerar cuando se instalen cámaras con finalidad personal o doméstica, con

fines de seguridad pública, en el ámbito de la actividad bancaria, en el ámbito laboral, en edificios y complejos habitacionales, en Entidades Públicas, en instituciones educativas y primarias y cuando se instalen en drones.[1]

Videovigilancia en ambulancias comunes, especiales y camionetas con accesibilidad

Mediante Dictamen N° 1/021, de 23 de febrero de 2021, se dictamina sobre consulta presentada por el Banco de Previsión Social. Se expresa que los datos personales que se tratarán en esta contratación son datos de salud de los pacientes (arts. 4° y 18 de la Ley N° 18.331), los que son especialmente protegidos. En ese sentido, debería monitorearse exclusivamente el ascenso y descenso del vehículo, pero no lo que sucede durante el traslado del paciente, por tratarse de datos sensibles.

En atención a lo expresado, el monitoreo por 3 cámaras en cada vehículo (considerando además la exigencia de una de ellas en el interior del vehículo en el caso de la camioneta de accesibilidad), adicionalmente a un sistema de rastreo, resulta desproporcionado a la finalidad perseguida.

En cuanto a quién es el responsable de la base de datos, conforme el artículo 4° lit. K) de la Ley N° 18.331, dicho rol corresponde al consultante, ya que es quién decide sobre la finalidad, contenido y uso del tratamiento de la información, por tratarse de sus pacientes. Se debe distinguir esa base de datos de la de las otras instituciones que comparten el servicio de traslado.

En caso de colocación de cámaras de video-vigilancia que recolecten datos sensibles no resulta suficiente la señalética, por cuanto el tratamiento de estos datos debe ser previo, expreso y escrito (artículo 18 de la Ley N° 18.331). [2]

Utilización de cámaras para perfilamiento comercial

Mediante Dictamen N° 3/021, de 23 de marzo de 2021, se informa respecto a un proyecto basado en utilizar las imágenes captadas por las cámaras de videovigilancia instaladas en locales comerciales para, mediante un proceso de disociación de datos que utiliza inteligencia artificial, obtener información de tipo estadístico sobre comportamientos generales dentro del local.

Las imágenes obtenidas por las cámaras no son almacenadas a estos efectos, ni por el cliente ni por el desarrollador del sistema, ya que una vez captadas ingresan en forma inmediata a un proceso de disociación siendo imposible revertirlas de modo de saber a qué persona corresponde al dato genérico obtenido. Se aclara que la información disociada será enviada a una nube en un país con estándares adecuados en materia de protección de datos y se observarán las medidas de seguridad necesarias para que los datos personales no puedan ser revertidos u obtenidos por terceros no autorizados.

El tratamiento realizado en este caso no tiene como fin la videovigilancia en el sentido de seguridad privada, ni tiene una finalidad conexa a ella, por lo que no resulta viable utilizar los logos de videovigilancia como medio de informar, en tanto la población reconoce que estos logos se implementan con fines de seguridad, lo que lleva a que las personas de por sí entiendan que solamente existe un tratamiento de los datos con esta finalidad (artículo 8° de la Ley).

En el marco de la responsabilidad proactiva (artículo 12 de la Ley), se deberán desarrollar medios efectivos y fácilmente diferenciables para que las personas conozcan de la existencia de este tratamiento. Asimismo, se debe contar con medios efectivos para el ejercicio del resto de los derechos de la protección de datos personales. Se debe determinar además el tiempo de conservación de este tipo de información conforme con el principio de finalidad (artículos 7° y 8° de la Ley).

El propietario de la información y quien dispone de los datos personales para realizar el tratamiento es el propietario del local, responsable del tratamiento de acuerdo con lo dispuesto en el art. 4° literal k) de la Ley N° 18.331. Por ende, deberá proceder a inscribir un registro de base de datos en forma independiente al de videovigilancia en tanto se trata de una finalidad distinta debiendo en el registro consignar especialmente la procedencia de los datos, el tiempo de conservación de éstos y la existencia de encargados de tratamiento

1 Acceder a la Resolución N° 58/021 sobre el uso de cámaras de videovigilancia en diversos ambientes.

2 Acceder al Dictamen N° 1/021

En cuanto al proceso de disociación se indica que según el literal g) del art. 4° de la Ley N° 18.331 se trata de "*todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable*". En tanto la disociación puede ser un proceso reversible, se deben realizar auditorías periódicas que aseguren que no se pueda revertir efectivamente. En lo que hace relación con las medidas de seguridad, se debe tener en cuenta que las mismas tienen que evitar la pérdida o adulteración de los datos personales. Además, si el tratamiento se enmarca dentro de algunas de las causales del Decreto N° 64/020, de 17 de febrero de 2020, se debe proceder a realizar una evaluación de impacto y eventualmente designar un delegado de protección de datos. Se debe verificar el cumplimiento con carácter general de toda la normativa de protección de datos personales. [3]

Sobre la normativa de lavado de activos y la protección de datos personales.

Mediante Dictamen N° 5/021, de 13 de abril de 2021, se resuelve consulta sobre el alcance de la Ley N° 19.574, de 20 de diciembre de 2017, y su decreto reglamentario con relación a las normas en protección de datos.

Del estudio de estas normas no se desprende que exista una regulación especial de las bases de datos de los clientes que han sido analizados con respecto al cumplimiento de las normas en materia de lavado, sino un régimen especial de tratamiento de los datos que pretende establecer determinadas obligaciones a los sujetos obligados en aras de dar cumplimiento a la finalidad de la norma, que es la prevención del lavado de activos.

Ha sido un criterio firme de esta Unidad exceptuar de la aplicación de la norma únicamente aquellos casos en los cuales existe una ley especial que crea y regula las bases de datos. En este caso, existe sí un tratamiento asociado a disposiciones específicas del sector, al igual que por ejemplo en la salud, pero ello no implica que opere la excepción citada del literal c) del artículo 3° de la Ley N° 18.331.[4]

Ámbito de aplicación de la Ley a actividades de alojamiento en territorio nacional.

Mediante Dictamen N° 10/021, de 8 de junio de 2021, se presenta consulta referida al ámbito de aplicación de la Ley a actividades de alojamiento en territorio nacional. Se consulta respecto a una empresa extranjera que proyecta contratar servicios de housing y conectividad en su centro de datos, sin acceder ni procesar información. El consultante entiende que la situación encuadra dentro de la excepción del artículo 37 lit. C) de la Ley N° 19.670, de 15 de octubre de 2018, por lo que a su entender sólo debería designar un representante con domicilio en Uruguay.

El consultante agrega que el inciso 2° del art. 2° del Decreto N° 64/020, de 17 de febrero de 2020 excepciona únicamente de la obligación de registro de las bases de datos, por lo que, para el caso referido, plantea si la empresa estaría excepcionada de la aplicación de toda la Ley N° 18.331, de 11 de agosto de 2008, o solamente de la inscripción en el registro. A efectos de contar con la información pertinente, se solicitó al consultante que indicara si la empresa realiza oferta de bienes y servicios dirigidos a habitantes de la República, o si las actividades de tratamiento de datos están relacionados con el análisis de su comportamiento, lo que fue contestado en forma negativa.

El artículo 37 de la Ley N° 19.670, establece que el tratamiento de datos personales está sometido a la Ley N° 18.331, modificativas y concordantes, cuando se efectúe por un responsable o encargado de tratamiento establecido en territorio uruguayo, lugar donde ejerce su actividad, siendo ésta la regla general. La disposición citada regula otras situaciones en las que se aplica la Ley N° 18.331, entre ellas la del tratamiento realizado por medios situados en el país. La excepción se produce cuando los medios se utilicen exclusivamente con fines de tránsito, y para este caso puntual la norma requiere que el responsable del tratamiento designe un representante, con domicilio en territorio nacional, ante esta Unidad a fin de cumplir con las obligaciones previstas por la Ley N° 18.331.

De conformidad con el artículo 1° literal d) del Decreto N° 64/020, se entiende por medios situados en el país la existencia de redes de información y de comunicación, centro de datos e infraestructura informática en general, entre otros. No existe una definición normativa de "*en tránsito*" pero refiere a casos en los que la información no se encuentra alojada en

3 Acceder al Dictamen N° 3/021

4 Acceder al Dictamen N° 5/021

el país, sino que transita de un punto a otro, pasando en su camino por el territorio nacional.

En la medida que se realiza hosting y conectividad en el prestador del servicio en territorio nacional, aun cuando no exista una actividad de tratamiento fuera del propio almacenamiento contratado –que de por sí es un tratamiento de datos-, de acuerdo con el Decreto mencionado se estaría ante un caso de utilización de "*centro de datos*" o "infraestructura informática en general", y no con fines de tránsito.

Por tanto, corresponde se dé cumplimiento a lo dispuesto en el artículo 2° del Decreto N° 64/020, que establece que los responsables y encargados de tratamiento, en su caso, deberán dar cumplimiento a las obligaciones previstas en la Ley N° 18.331 y modificativas, incluyendo el registro de sus bases de datos.[5]

Sobre la historia clínica laboral

Mediante Dictamen N° 12/021, de 29 de junio de 2021, se analiza desde la perspectiva de protección de datos personales la historia clínica laboral.

En base al marco normativo considerado es correcto el mantenimiento de una historia clínica laboral, la que debe contemplar aquellos aspectos de salud de los trabajadores que puedan incidir en lo que tiene relación con el desarrollo de su tarea.

Se considera que los datos que obren en la historia clínica deberán ser los imprescindibles para el cometido fijado y ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados, los que no podrán ser además comunicados entre bases de datos, sin que medie ley o consentimiento previo de titular.

Con respecto al contenido de la información de la historia clínica laboral, ésta debe utilizarse solamente para el control de aquellas enfermedades que puedan afectar la relación laboral, teniendo en cuenta el alcance indicado por el Convenio N° 161 de la OIT. A ello se debe agregar que los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

Por su parte, la información que se encuentre en la historia debe ser proporcionada en forma expresa por el titular no estando habilitada la obtención de información de terceros distintos al titular, con excepción, para casos concretos, de obtener datos de antecedentes familiares, sobre todo cuando se trata de enfermedades de carácter hereditario.

Se recomienda la imposición de niveles de acceso a los contenidos de la historia clínica laboral, además de la necesaria adopción de medidas de seguridad suficientes que eviten la adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Asimismo, se indica que después de finalizada la relación laboral, se podrá conservar la información en tanto existan obligaciones legales, pero en este caso la información deberá estar bloqueada de forma que se impida su tratamiento.

Se agrega que tratándose de datos de salud (sensibles de conformidad con lo establecido en el art. 4° literal e) de la Ley N° 18.331), se deberán implementar medios para recabar el consentimiento que en el caso es expreso y escrito, considerando que la Ley N° 18.600, de 21 de setiembre de 2009 le reconoce a la firma electrónica avanzada la misma validez que la firma hológrafa.

Además, deberá procederse a la inscripción de las historias clínicas que se generen en el Registro que lleva adelante esta Unidad.

Por otra parte, resulta necesaria la adopción de medidas de responsabilidad proactiva, la realización de una evaluación de impacto y la designación de un delegado de protección de datos personales (arts. 5°, 6° y 10° del Dec. 64/020).

En cuanto a la posibilidad de realizar estadísticas con la información obrante en las historias clínicas, se deberá estar a la necesidad y proporcionalidad de dicha tarea, además de implementar criterios de disociación que permitan la total eliminación de datos que puedan identificar a las personas.[6]

5 Acceder al Dictamen N° 10/021

6 Acceso Dictamen N° 12/021

Sobre la información a proveer en convenios de colaboración de investigación médica.

A través del Dictamen N° 14/021, de 6 de julio de 2021, se dictamina sobre a información que se debe proveer en convenios de colaboración de investigación médica.

Se indica que en forma previa a llevar a cabo la investigación se debe dar cumplimiento al art. 13 de la Ley N° 18.331 y brindar información sobre los aspectos allí establecidos a las personas que formen parte de esta. Esta información además deberá contar con los requerimientos establecidos en el N° 158/019, de 12 de junio de 2019 sobre los aspectos a explicitar a los intervinientes en proyectos de investigación.

Además, los datos recolectados y tratados en el marco del Convenio presentado se regulan por los artículos 18 y 19 de la Ley N° 18.331, por lo que se requiere el consentimiento expreso y escrito del titular de los datos, y que el tratamiento sea realizado por las propias instituciones relacionadas con los datos de salud.

En cuanto al consentimiento éste deberá documentarse, siendo responsable en este caso la Facultad de Medicina de la Universidad de la República tanto de informar a las personas como de recabar su consentimiento con las citadas características. Este consentimiento también deberá recabarse cumpliendo con los requerimientos establecidos en el Decreto N° 158/019.

Asimismo, se debe informar a los participantes que se realizará una transferencia internacional de datos, y disociarlos antes de ser transferidos, aplicando criterios de disociación que aseguren la imposibilidad de su reversión.

En caso de que las transferencias se realicen a Estados Unidos con información nominada, para estas se debe contar con el consentimiento del titular de los datos, obtenido en forma previa. En caso de que los datos sean transferidos a una nube segura, deberá conocerse en forma previa los requisitos de seguridad ofrecidos por el proveedor, los que deben cumplir con la Ley N° 18.331.

En lo que refiere a la remisión de información a una casilla de correo electrónico institucional, el tratamiento de datos debe realizarse de forma tal que se conserve la integridad y disponibilidad de la información (artículo 10 de la Ley N° 18.331).

Además, se deberá proceder a la eliminación de la información una vez agotada la finalidad del convenio (artículo 8° de la Ley N° 18.331) por lo que se sugiere la definición concreta de este aspecto en el protocolo que se debe diseñe a los efectos de la investigación.

El Dictamen expresa que en el caso se deberá proceder a realizar la inscripción de la base de datos que se genere en su calidad de responsable de tratamiento (artículo 6° de la Ley N° 18.331). En su calidad de responsable, se recomienda revisar la cláusula 5 del Anexo de transferencia de materiales sobre responsabilidad de las partes.

La evaluación de impacto prevista en el artículo 6° del decreto N° 64/020, de 17 de febrero de 2020 debe realizarse en forma previa a la investigación y a la transferencia internacional de datos.[7]

Intercambio de información entre Entidades Públicas

Mediante Dictamen N° 17/021, de 10 de noviembre de 2021, se emite Dictamen sobre consulta realizada por una institución pública sobre información solicitada por el Instituto Nacional de Estadística.

En el presente caso se trata de datos personales de funcionarios públicos solicitados a los efectos de confeccionar un índice por parte de la entidad pública con cometidos para ello, siendo de aplicación las Leyes N° 16.616, N° 18.331, y N° 18.381 de 17 de octubre de 2008.

El Índice Medio de Salarios fue creado por el artículo 39 Ley N° 13.728, de 17 de diciembre de 1968, y es llevado por el INE como una de sus funciones desde el dictado del decreto N° 26/969, de 14 de enero de 1969 (norma posteriormente derogada y sustituida).

De conformidad con lo indicado se trata en el caso de una comunicación de datos, amparada por el literal B del artículo 9° por remisión del literal B del artículo 17 de la Ley N° 18.331, por lo que no es necesario para la comunicación de los datos

7 Acceder al Dictamen N° 14/021

indicados en la consulta, del previo consentimiento informado. Por otra parte, con respecto a los datos comunicados, rige el secreto estadístico establecido en el artículo 3° de la Ley N° 16.616.

No obstante lo indicado, corresponde señalar que la ley N° 18.331 –posterior en el tiempo a la Ley N° 16.616, y comprensiva de un régimen general instituido para la protección del derecho humano fundamental a la protección de datos personales- establece un conjunto de principios y obligaciones que deben cumplir todas las entidades públicas que traten datos personales, incluyendo al INE.

En ese sentido, debe prestarse especial atención a lo establecido en el art. 12 de la Ley N° 18.331, en la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018, y en el decreto N° 64/020, de 17 de febrero de 2020, acerca de la adopción de mecanismos de responsabilidad proactiva que incluyan la privacidad por defecto, la privacidad por diseño y las evaluaciones de impacto, adicionalmente a la designación de un delegado de protección de datos, de conformidad con el artículo 40 de la última de las leyes citadas.[8]

Interpretación del art. 37 de la ley N° 19.670

A través del Dictamen N° 19/021, de 1° de diciembre de 2021, se emite opinión respecto a la consulta presentada por un estudio jurídico sobre interpretación del artículo 37 de la Ley N° 19.670 que modificó el ámbito territorial de la normativa de protección de datos personales.

En el caso se indica al consultante que la normativa de protección de datos personales se aplica a las personas físicas y a las personas jurídicas "*en cuanto corresponda*".

En ese marco, si un responsable de tratamiento ubicado fuera del país ofrece bienes o servicios exclusivamente a personas jurídicas constituidas en Uruguay, le será aplicable la normativa uruguaya de protección de datos en cuanto corresponda. Sobre el alcance de cuándo "*corresponde*" la aplicación de la normativa se deberá estar las características de caso concreto y, en su caso, al criterio emitido por esta Unidad en ejercicio de lo previsto por la ley N° 18.331 de 11 de agosto de 2008, art. 34, en especial su literal "A". [9]

Recomendaciones para el uso de aplicaciones móviles con tratamiento de datos sensibles

Por Dictamen N° 20/021, de 1 de diciembre de 2021, se brindan recomendaciones para el uso de aplicaciones móviles que se dedican al tratamiento de datos sensibles.

En este sentido, la consultante expresa que mediante una determinada aplicación se hace un seguimiento de ejercicios con bandas elásticas o elementos inextensibles y se utiliza para la rehabilitación mediante un seguimiento de la mejora progresiva de la fuerza y velocidad del paciente. Indica la empresa que también se pretende utilizar en el ámbito deportivo para realizar ejercicios que imitan el gesto deportivo.

En el caso se indica que, si el dispositivo es utilizado en el marco de telemedicina, la empresa se convierte en un encargado de tratamiento siendo la institución médica la responsable y quien debe dar cumplimiento a las obligaciones legales. En esta hipótesis se recomienda la adopción de un contrato con las instituciones que utilizarán el dispositivo para determinar los derechos y obligaciones de cada parte. En cambio, si dispositivo es utilizado directamente por la persona, entonces la empresa será responsable, con las correspondientes obligaciones asociadas.

Conforme con lo detallado en relación con la consulta, se recopilarán datos personales tanto generales (nombre, edad, género altura y masa) como sensibles (datos de rehabilitación). De acuerdo con el principio de legalidad indicado en el artículo 6° de la Ley N° 18.331, de 11 de agosto de 2008, se debe proceder a la inscripción de las bases de datos que se generen.

En cuanto al alojamiento de la información se deberá dar cumplimiento al artículo 23 de la citada Ley. En este sentido se ha puesto en conocimiento de esta Unidad que "*Se utilizará una base de datos de AWS (Amazon) en un país bajo las*

8 Acceder al Dictamen N° 17/021

9 Acceder al Dictamen N° 19/021

"Standard Contractual Clauses", *en principio en Alemania o Canadá. Esta base de datos almacenará tanto la información del usuario como de las sesiones realizadas"*. En este sentido la transferencia se basa en cláusulas contractuales tipo por lo que se encuentra amparada por la normativa vigente, siempre que sean presentadas y aprobadas por la Unidad.

De acuerdo con el artículo 9° de la Ley, se requiere recabar el consentimiento de los titulares en forma libre, previa, expresa e informada y debe ser documentado. Este aspecto también se encuentra contemplado dentro de las previsiones del responsable, en tanto indica que el consentimiento en todos los casos debe ser firmado en forma previa al uso de la aplicación. Si se trata de una relación donde MOVI es la encargada el registro debe ser llevado por el responsable, excepto que contractualmente se estipule de otra forma. Si MOVI es responsable debe ser quien lleve el registro de los consentimientos. Deberán cumplirse además con los restantes principios en materia de protección de datos personales (artículos 7° y 8° de la Ley N° 18.331), y en especial el artículo 10 (seguridad de los datos).

Además, se requiere la incorporación de una política de privacidad que explique el tratamiento de datos personales y el cumplimiento de la normativa de protección de datos personales. Este aspecto ya se encuentra abordado por el consultante, recomendándose que ésta se aplique no sólo cuando la aplicación se utiliza en el marco de telemedicina por prescripción médica y bajo la responsabilidad de la institución de salud, sino también cuando MOVI es responsable de tratamiento.

En lo que respecta a los derechos de los titulares (artículos 13 a 16), se recomienda la adopción de procesos internos que permitan el ejercicio de estos derechos o coordinados con el responsable que utilizará la aplicación.

En forma complementaria se recuerda que, más allá de estos aspectos concretos, se deberá dar cumplimiento a toda la normativa de protección de datos personales con carácter general, en especial por el tipo de datos tratados, aquellas vinculadas a la responsabilidad proactiva (artículo 12 de la Ley N° 18.331, en la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018, y decreto N° 64/020, de 17 de febrero de 2020). [10]

Empresas de videovigilancia situadas en el exterior

Por Dictamen N° 22/021, 14 de diciembre de 2021, se expresa este Consejo sobre las empresas que prestan servicios de videovigilancia y realizan tratamiento de datos personales de sus clientes y de las personas que son captadas por sus sistemas serán considerados responsables o encargados según lo dispuesto en los literales H y K del art. 4° de la Ley N° 18.331, de 11 de agosto de 2008.

En cualquiera de los casos –responsables o encargados-, aun cuando se encuentren fuera del territorio nacional, se encuentran sometidos a la ley uruguaya en las hipótesis previstas en el art. 37 de la Ley N° 19.670, de 15 de octubre de 2018. En el caso concreto, a través de la prestación de un servicio para habitantes del Uruguay.

El artículo 2° del decreto N° 64/020, de 17 de febrero de 2020 indica que los responsables y encargados de tratamiento, en su caso, deberán dar cumplimiento a las obligaciones previstas en la Ley N° 18.331, incluyendo el registro de sus bases de datos y brindando la información de contacto correspondiente ante la Unidad Reguladora y de Control de Datos Personales.

En el caso de que la empresa de seguridad en el exterior actúe como encargada de tratamiento, el responsable en territorio nacional deberá además proceder a la inscripción o actualización de la base de datos correspondiente, señalando tal extremo.

El alojamiento de las bases de datos en una nube en el exterior constituye una transferencia internacional de datos, por lo que deberá estarse al régimen dispuesto en el art. 23 de la Ley N° 18.331 y la Resolución N° 23/021 de este Consejo Ejecutivo.[11]

10 Acceder al Dictamen N° 20/021

11 Acceder al Dictamen N° 22/021

Avances normativos

Desde el punto de vista legislativo, merece especial atención en el año 2021, la *promulgación de la Ley N° 19.948, de 16 de abril de 2021, por la que se aprueba el Protocolo de Enmienda del Convenio para la protección de las personas con respecto al tratamiento de datos personales, suscrito en Estrasburgo.*

El protocolo de enmienda, conocido como convenio 108+ ya fue objeto de diversas notas por parte de la doctrina y de la propia Unidad, y se constituye en un instrumento fundamental para estrechar los lazos de colaboración entre distintos países y organizaciones a lo largo del mundo, en el tema de protección de datos.

Actualmente existen 19 países que han internalizado sus disposiciones, siendo necesario para su entrada en vigencia plena la ratificación por todas las partes, o que al 11 de octubre de 2023 haya sido ratificado por al menos 38 de estas.

En lo que refiere a disposiciones legislativas con especial impacto en la protección de datos personales, debe destacarse la promulgación de la Ley N 19.996, de 3 de noviembre de 2021, que en su artículo 181 crea en el ámbito de la Unidad Reguladora de Servicios de Comunicaciones (URSEC) el denominado "Registro Nacional No Llame", con el objetivo de proteger a los titulares o usuarios de servicios de telecomunicaciones, de abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados. Esta protección se agrega a la ya establecida en la Ley N° 18.331, de 11 de agosto de 2008 para la recepción de publicidad no deseada, y el ejercicio de los derechos previstos en la propia ley, lo que requerirá sin dudas un trabajo coordinado de la URSEC y la URCDP.

Desde la perspectiva de normatividad emanada de la propia Unidad, corresponde hacer hincapié en la modificación del régimen de transferencias internacionales, adaptando la resolución 4/019, de 12 de marzo de 2019 para invalidar el esquema "Privacy Shield" que habilitaba las transferencias a los Estados Unidos, y aprobar alternativas adecuadas a las necesidades de responsables y encargados. En ese sentido, se aprobaron las resoluciones 23/021, de 8 de junio de 2021 y 41/021, de 8 de setiembre de 2021, otorgándose un plazo para adaptarse a sus disposiciones.

Por la relevancia de las citadas disposiciones, se transcriben a continuación:

Resolución 23/021

Montevideo, 8 de junio de 2021.

VISTO: La necesidad de actualizar la Resolución Nº 4/019, de 12 de marzo de 2019, 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:

I. Que la resolución indicada en el Visto sustituyó la Nº 17/009, de 12 de junio de 2009, y estableció los territorios adecuados y en consecuencia apropiados para las transferencias internacionales de datos.

II. Que al efecto se consideraron las evaluaciones realizadas por la Unidad, y los casos en los que existe una protección equivalente a la uruguaya, sea por la pertenencia a determinada región o por la evaluación realizada por entidades especializadas en la valoración del ajuste de legislaciones nacionales a los principios y derechos vinculados a la protección de datos.

III. Que en función de los antecedentes citados, la Resolución N° 4/019 estableció que se consideran adecuados 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. Ello sin perjuicio de las limitaciones previstas en las correspondientes decisiones de adecuación emitidas por la Comisión Europea.

CONSIDERANDO:

I. Que la transferencia internacional de datos supone su transmisión fuera del territorio nacional y 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.

II. 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; y esta Unidad es el órgano encargado de establecer los países y organismos que brindan dichos niveles de protección.

III. Que en esa consideración, la Unidad ha tenido en cuenta especialmente los Estándares en Protección de Datos Personales para los Estados Iberoamericanos 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.

IV. Que los países miembros de la Unión Europea cumplen con los estándares internacionales por aplicación del citado Reglamento y, por otra parte, se estima que los terceros países u organizaciones que han sido objeto de decisiones de adecuación del Parlamento Europeo y el Consejo poseen un nivel adecuado de protección, al acompasar su normativa a la de dicho estándar internacional.

V. Que en el caso de los terceros países u organizaciones considerados adecuados, corresponde entenderse incluidas en la presente Resolución todas las limitaciones o excepciones previstas en la decisión correspondiente a que refiere el Considerando anterior.

VI. Que con respecto a la adecuación de las organizaciones incluidas en el marco del "Privacy Shield", existen elementos derivados del análisis del tratamiento de los datos en los Estados Unidos de América que llevaron a la invalidación de ese marco en el territorio europeo, los cuales justifican la revisión de la Resolución de esta Unidad. Esos elementos resultan en particular de la sentencia del Tribunal de Justicia de la Unión Europea de 16 de julio 2020.

VII. VII. Que, por lo mismo, las transferencias internacionales realizadas a los Estados Unidos de América deberán justificarse a través del consentimiento de los interesados o de alguna de las excepciones previstas en el artículo 23 de la Ley N° 18.331, y en su caso, contar con la autorización expresa de esta Unidad. A estos efectos se valorará especialmente la adopción de cláusulas contractuales apropiadas, la ubicación de los encargados de tratamiento en Estados que hayan adoptado normas tuitivas de la protección de datos y la adopción del esquema de auto-certificación puesto a disposición por la Federal Trade Commission, entre otros elementos.

VIII. Que se aprecia la necesidad de otorgar a los responsables y encargados de tratamiento que hubieran sustentado sus transferencias en el marco indicado en el Considerando VI un plazo para las adecuaciones necesarias.

ATENTO: A lo expuesto,

LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

RESUELVE:

1) Sustituir la Resolución Nº 4/019, de 12 de marzo de 2019, 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, 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 indicado en el Considerando V de esta Resolución.

3) Otorgar a los responsables y encargados de bases de bases o tratamiento que a la fecha de vigencia de la presente Resolución hayan fundado sus transferencias a Estados Unidos de América en el marco de "Privacy Shield", un plazo de seis meses para ajustar las condiciones de las transferencias realizadas, a contar desde la publicación de la presente resolución en el Diario Oficial.

4) Notifíquese, publíquese en el Diario Oficial y en la página web de la Unidad, y oportunamente archívese.

FIRMADO POR: **FELIPE ROTONDO TORNARÍA**
CONSEJO EJECUTIVO URCDP

Resolución 41/021

Montevideo, 8 de setiembre de 2021

VISTO Y CONSIDERANDO: Lo dispuesto por el artículo 23 de la Ley N° 18.331, de 11 de agosto de 2008 respecto a las transferencias internacionales a territorios no adecuados,

RESULTANDO:

I. Que, de conformidad con el artículo indicado, "*la Unidad Reguladora y de Control de Protección de Datos Personales podrá 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 derivarse de cláusulas contractuales apropiadas*."

II. Que, por Resolución N° 23/021, de 8 de junio de 2021, este Consejo Ejecutivo determinó los territorios considerados adecuados para la transferencia internacional de datos, así como instrumentos para brindar garantías a la protección de la vida privada que deben considerar los responsables, entre los que se encuentran las cláusulas contractuales apropiadas.

III. Que, en ese sentido, se estima pertinente adoptar una guía para la redacción de cláusulas contractuales que aseguren un contenido ajustado a las normas en materia de protección de datos personales, el que deberá complementarse con otros aspectos relativos a las operaciones de tratamiento que se pretendan realizar.

ATENTO: a lo expuesto e informado,

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

RESUELVE:

1) Recomendar a los responsables y encargados de tratamiento que pretendan realizar transferencias internacionales de datos en el marco del artículo 23 de la Ley N° 18.331, de 11 de agosto de 2008, la adopción de cláusulas contractuales como las indicadas en el Anexo I de la presente resolución.

2) NOTIFÍQUESE Y PUBLÍQUESE

FIRMADO POR: **FELIPE ROTONDO TORNARÍA**
CONSEJO EJECUTIVO URCDP

Anexo I a Resolución 41/2021 del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales

CONTENIDO MÍNIMO DE CLÁUSULAS CONTRACTUALES PARA TRANSFERENCIAS INTERNACIONALES A PAÍSES NO ADECUADOS [12]

ANTECEDENTES

En lo que respecta a las transferencias internacionales de datos a países no adecuados -de conformidad con la resolución indicada-, los responsables y encargados deben adoptar determinadas salvaguardas para asegurar la debida protección de datos de titulares, que son objeto de tratamiento.

En el marco de los mecanismos habilitantes de las transferencias, se encuentra la adopción de cláusulas contractuales que

12 Acceder a la Resolución N° 41/021

determinen claramente las responsabilidades de las partes involucradas.

El presente anexo presenta un contenido mínimo indispensable que deben contener los contratos a suscribir entre un responsable o encargado en territorio nacional con responsables o encargados situados fuera de éste. En primer lugar se presentan contenidos de cláusulas comunes a todas las transferencias y en los apartados siguientes contenidos específicos, adicionales a los primeros, según el tipo de emisor o destinatario.

La naturaleza del vínculo entre la parte exportadora e importadora de los datos determina la existencia de distintos tipos de obligaciones y responsabilidades que deben encontrarse claramente definidas. En esta definición, y de conformidad con lo establecido en el artículo 40 de la Ley N° 19.670, debe participar cuando corresponde, el delegado de protección de datos.

Por otra parte, la transferencia internacional, en tanto se realiza a territorio no adecuado, debe ser antecedida en todos los casos de una evaluación de impacto en la protección de datos, de conformidad con lo establecido en el artículo 6° literal f del decreto N° 64/020.

CLAUSULAS COMUNES A TRANSFERENCIAS ENTRE TODO TIPO DE IMPORTADOR Y EXPORTADOR DE DATOS

Finalidad – Se debe establecer claramente cuál es la finalidad que se persigue con la transferencia que se pretende realizar, sin perjuicio del detalle que se realice según se trate de transferencia a responsable o a encargado.

Normativa aplicable – En todos los casos debe preverse la aplicación de la normativa uruguaya, Leyes N° 18.331, de 11 de agosto de 2008, N° 19.670, de 15 de octubre de 2018, decretos N° 414/009, de 31 de agosto de 2009 y N° 64/020, de 17 de febrero de 2020, normas modificativas y concordantes.

Definición de los términos de protección de datos aplicables – Deben definirse los términos más comunes aplicables a la regulación de la transferencia, remitiéndose a las definiciones previstas legal y reglamentariamente, en lo pertinente (artículos 4° de la Ley N° 18.331 y 4° del decreto N° 414/009). En especial no debe omitirse la definición de importador, exportador, responsable, encargado, sub-encargado, titular del dato, dato personal y tratamiento.

Contenido de la transferencia – Deberá detallarse el listado de datos transferidos con la mayor exactitud y completitud posible. En caso de datos sensibles, deberá en lo posible detallarse adicionalmente el contenido y propósito para la transferencia de cada dato.

Transferencias posteriores – Establecer, en caso de corresponder, las condiciones para habilitar transferencias posteriores de información desde el destino del importador, que en todos los casos deberán cumplir con la normativa habilitante (artículo 23 de la Ley N° 18.331).

Derecho de información – En todos los casos deberán explicitarse los contenidos mínimos previstos en el artículo 13 de la Ley N° 18.331. Adicionalmente, deberá incluirse la identificación de los encargados y sub-encargados de tratamiento, cuando corresponda. La información deberá estar disponible en forma permanente o a solicitud del titular del dato, según corresponda.

Operaciones de tratamiento – En todos los casos deberán identificarse las operaciones de tratamiento específicas a realizar y las medidas operativas y de seguridad necesarias para dar cumplimiento al principio de seguridad de los datos y de responsabilidad proactiva (artículos 10 y 12 de la Ley N° 18.331, este último en la redacción dada por el artículo 39 de la Ley N° 19.670, y decreto N° 64/020).

Resolución de disputas – Podrán preverse mecanismos específicos para la resolución de disputas, pero ello de ningún modo podrá alterar las operaciones de tratamiento que son de interés del titular del dato, o afectar de modo alguno sus derechos, o suponer un incumplimiento de la normativa aplicable, o que establezcan una retención indebida de información que de conformidad con la normativa aplicable deba ser suprimida.

Autoridad de control administrativa – En todos los casos deberá preverse que la autoridad de control para el caso de determinación de incumplimientos será la autoridad uruguaya, salvo en caso de incumplimientos específicos del importador del dato que se encuentren sujetos al contralor de la autoridad homónima en el país de destino. Ello sin perjuicio de la aplicabilidad, en su caso, del artículo 37 de la Ley N° 19.670 y artículos 1° y 2° del decreto N° 64/020.

Cumplimiento de medidas de responsabilidad proactiva previas – En todos los casos deberá agregarse en forma de anexo la Evaluación de Impacto en la Protección de Datos de carácter obligatorio de conformidad con el artículo 6° literal f del decreto N° 64/020.

Resguardo de documentación – Deberán establecerse las condiciones para el resguardo de la documentación tanto por el importador como por el exportador y otros interesados (como por ejemplo eventuales sub-encargados), la que deberá conservarse en la forma establecida en el artículo 5° del decreto 64/020, y estar a disposición de la Unidad de conformidad con el artículo 34 literal D de la Ley N° 18.331.

Confidencialidad – Establecer el contenido de las obligaciones de confidencialidad asumidas por el personal del importador y el exportador.

Acceso a información por autoridades extranjeras – Deberá preverse que sólo podrá accederse a información en el destino del importador del dato por parte de autoridades del tercer país en el marco de normas legales vigentes que otorguen las debidas garantías a los titulares de los datos y con orden judicial. En todos los casos deberán tomarse las medidas para que el acceso no se realice a todos los datos sino únicamente a los estrictamente necesarios para el cumplimiento de la orden judicial correspondiente. Deberá preverse que se brinde al responsable situado en territorio nacional información de la solicitud en forma inmediata, en los casos en que ello sea posible; en caso contrario deberá brindarse la información en la primera oportunidad posible.

CLÁUSULAS ESPECÍFICAS APLICABLES A TRANSFERENCIAS ENTRE RESPONSABLES Y RESPONSABLES

Base de legitimación para la comunicación – Deberá justificarse la aplicación de alguna de las causales previstas en el artículo 17 de la Ley N° 18.331, por tratarse de una comunicación de datos.

Base de legitimación para el tratamiento previsto – Deberá justificarse la aplicación de alguna de las causales previstas en el artículo 9° o 18°, y concordantes, de la Ley N° 18.331, para el tratamiento que se pretende realizar.

Responsabilidad solidaria – Remarcar la responsabilidad solidaria aplicable de conformidad al artículo 17 de la Ley 18.331 para la comunicación de datos, lo que en ningún caso podrá implicar que se prohíba la reclamación correspondiente por parte del titular del dato al responsable situado en territorio nacional.

Contratación de encargados de tratamiento – Deberán preverse las condiciones para la contratación de encargados de tratamiento por el importador de los datos, dando cumplimiento en lo pertinente, a las condiciones previstas en las cláusulas que siguen.

Comunicación de vulneraciones de seguridad – Deberá preverse un mecanismo de comunicación de vulneraciones de seguridad a los titulares de los datos y a la Unidad dando cumplimiento a las condiciones y plazos previstos en el artículo 38 de la Ley N° 19.670 y artículos 3° y 4° del decreto N° 64/020.

CLÁUSULAS ESPECÍFICAS APLICABLES A TRANSFERENCIAS ENTRE RESPONSABLES Y ENCARGADOS

Retención y supresión de información – Deberá establecerse el plazo específico de conservación de la información –que no podrá exceder el determinado por el propósito den encargo- y los medios para su devolución y supresión. Ello sin perjuicio de lo establecido en el inciso segundo del artículo 30 de la Ley N° 18.331.

Comunicación de vulneraciones de seguridad – Deberá preverse un mecanismo de comunicación inmediata al responsable de eventuales vulneraciones de seguridad. Eventualmente, podrá establecerse la obligación de comunicación directa a la URCDP.

Contratación de sub-encargados – Deberá prohibirse la contratación de sub-encargados salvo autorización expresa del responsable, lo que deberá además informarse en forma fehaciente a los titulares de los datos.

Ejercicio de derechos por los titulares – Deberán preverse mecanismos para la respuesta al ejercicio de derechos ante los encargados por parte de los titulares de los datos.

Responsabilidades – No podrá eximirse al responsable de su responsabilidad por la actuación del encargado, de conformidad con lo establecido en el artículo 12 de la Ley N° 18.331, sin perjuicio de la responsabilidad directa que pueda caberle a este último en caso de vulneración a lo preceptuado en la normativa vigente.

CLÁUSULAS ESPECÍFICAS APLICABLES A TRANSFERENCIAS ENTRE ENCARGADOS Y ENCARGADOS

Habilitación – La transferencia a otros encargados debe realizarse en el marco de un contrato previo con el responsable, y con los límites en él establecidos, el que deberá adjuntarse como anexo o referenciarse en las cláusulas correspondientes. Dicho contrato deberá contener como mínimo, las previsiones expresadas en el presente anexo para los contratos entre responsables y encargados, las que deberán extenderse a los sub-encargados en lo pertinente.

Si bien estas cláusulas deberán emplearse de principio para las transferencias a territorios no adecuados que no se enmarquen en alguna de las restantes hipótesis habilitantes del artículo 23 de la Ley N° 18.331, se exhorta su aplicación a todo tipo de transferencia internacional, en lo pertinente.

Guías de protección de datos personales

Guía general de protección de datos personales en Uruguay

Esta guía orienta sobre el Derecho a la Protección de Datos Personales y los medios para facilitar su ejercicio, y espera constituirse en una herramienta de capacitación útil para todas las personas.

La protección de datos personales es un derecho humano regulado en diversos instrumentos internacionales. En nuestro país, la Ley N° 18.331, de 11 de agosto de 2008, reconoce la protección de datos personales como un derecho fundamental incluido en nuestra Constitución, crea la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP) como el órgano que garantiza este derecho -con competencias necesarias para garantizar el cumplimiento de la normativa vigente-, e instituye un régimen basado en principios y derechos que se analizarán más adelante en este documento.

Acceder a la Guía general de Protección de Datos Personales en Uruguay.

Guía para el cumplimiento de obligaciones por entidades extranjeras

Los destinatarios de esta guía son los responsables y encargados de tratamiento que se encuentran situados fuera del territorio nacional, pero incluidos dentro del alcance "extraterritorial" de la normativa en protección de datos personales uruguaya. En primer lugar, resulta necesario distinguir los conceptos de responsable y encargado de protección de datos personales. En el ordenamiento jurídico uruguayo, el responsable de tratamiento es aquella persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento (literal k artículo 4° de la Ley N° 18.331, de 11 de agosto de 2008). Por su parte, encargado de tratamiento es aquella 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 (literal h del art. 4° de la Ley N° 18.331, de 11 de agosto de 2008).

Quienes son responsables y encargados y se encuentran fuera del territorio nacional se encontrarán sometidos a la ley uruguaya, en caso de encontrarse dentro de alguna de las situaciones previstas en el artículo 37 de la Ley N° 19.670, de 15 de octubre de 2018, las que se desarrollarán en el apartado 3 de esta guía.

Acceder a la Guía para el cumplimiento de obligaciones por entidades extranjeras

Guía para la gestión, documentación y comunicación de vulneraciones de seguridad en datos personales

Esta guía está orientada a los responsables y encargados de bases de datos o de tratamiento de datos personales según lo establecido en el artículo 4° lit. D de la Ley N° 18.331. Esto es, a quienes traten información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables y que pueden verse afectadas por brechas o incidentes de seguridad.

Acceder a la Guía para la gestión, documentación y comunicación de vulneraciones de seguridad en datos personales

Jurisprudencia Nacional

En cuanto al dictado de sentencias en materia de protección de datos personales resulta de interés citar dos casos sometidos a nuestros tribunales.

En primer lugar, la sentencia N° 60, de 19 de octubre de 2021, dictada por el Juzgado Letrado de Primera Instancia en lo Civil de 2° Turno, procedimiento realizado a través de una acción declarativa.

En estos autos los actores entablan esta acción contra Google Argentina S.R.L. y contra Google Inc. a efectos de que se reconozca el derecho a la supresión de sus datos personales sobre determinadas publicaciones en Internet en base al Dictamen realizado por la Unidad Reguladora y de Control de Datos Personales.

Indican que dos personas que trabajaban en su casa presentaron una denuncia por un supuesto delito de contratación en régimen de esclavitud y además se lo vinculaba con delitos relacionados con la trata de personas. Este procedimiento fue archivado a solicitud del Ministerio Público con fecha posterior pero este hecho tuvo gran difusión en los medios de comunicación en virtud de las partes involucradas.

En términos generales, la sede considera que lo que se pretende con el accionamiento impetrado es la desvinculación de los datos de la persona que se estiman inadecuados, obsoletos, erróneos y así dificultar la vinculación entre una determinada persona y la información publicada. En base a ello se entiende que no es procedente la falta de legitimación que alega Google respecto a la acción presentada.

La sentencia además releva la opinión del órgano de control ante un oficio enviado a éste en la que se destaca que se expresó que "…*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… sostener que los motores de búsqueda pueden ser considerados responsables del tratamiento. El hecho de que brinden opciones para la supresión o eliminación de información coadyuva en dicha interpretación.*

En el caso específico de 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…" (fs. 573).

En cuanto al fondo del asunto expresa que en Uruguay la protección de datos personales es un derecho humano comprendido en el art. 72 de la Constitución de la República conforme lo indica el artículo 1° de la Ley N° 18.331 refiriendo en forma complementaria al reconocimiento en diversos instrumentos internacionales. Asimismo, se hace referencia a que Uruguay forma parte del Convenio 108 y de su versión modernizada.

Según la sede "*El 'derecho al olvido', ha sido considerado por la doctrina como "la facultad que posee el titular de determinada información de carácter personal de solicitar que se elimine la misma de una base o fichero de datos porque ésta es obsoleta y por ello su publicación puede atentar contra su honor, su privacidad, su intimidad o menoscabar cualquier otro derecho fundamental que le asiste"*.

Es de destacar además que agrega que "*El hábeas data (en sentido amplio y no solo como acción judicial), en este caso cancelatorio, incide en datos que no procede mantener por razones que pueden ser de tiempo, cambio de finalidad, falsedad, revocación de un necesario consentimiento para el tratamiento, situaciones en que este no es legítimo; sería, entonces, un hábeas internet*"

Además indica que "*En efecto, si bien la Ley No. 18.331 no refiere expresamente al mismo, los derechos a solicitar la supresión, actualización, rectificación, etc. de los datos personales, son propios e inherentes de cada persona y por consiguiente, su ejercicio está permitido, tanto por los lineamientos de la propia norma como a poco tengamos en cuenta la autoejecutividad del derecho en el marco de lo dispuesto por el art. 332 de la Constitución Nacional, (…)*"

Sobre el caso concreto la Sede entiende que los hechos a los que refieren las publicaciones afectan los derechos del honor, la privacidad y la dignidad de los actores en tanto se les señala como responsables de delitos violatorios de derechos humanos. Indica además que no existe vulneración al derecho a la información y a la libertad. Tampoco existe un interés público en mantener la indexación de las respuestas que vinculan a los actores.

En definitiva, se expresa que "*les asiste a los actores el derecho a obtener la protección de sus datos personales mediante la desindexación o eliminación de los resultados de búsqueda de los enlaces que refieren a noticias que los vinculan a la denuncia penal tramitada en los autos IUE 474-98/2012, relacionados en su escrito*". En síntesis, declara que los actores tienen derecho a la desvinculación de sus nombres de los sitios denunciados y condena a Google LLC y a Google Argentina SRL a realizar la desindexación y desvinculación de la lista de resultados de su buscador (Google Search) de los datos personales de los actores respecto de las noticias publicadas en los sitios web señalados.

El otro caso de interés a citar es la Sentencia N° 173, de 21 de diciembre de 2021, dictada por el Tribunal de Apelaciones en lo Civil de 7° Turno. En este caso se resuelve una apelación sobre una sentencia que rechaza una acción de amparo contra Google LLC y otros.

En estos autos el objeto de la acción es el examen de lo sucedido respecto a una nota de los actores de fecha 1 de junio de 2017 que se encuentra disponible en la página de Sudestada. El 25 de octubre de 2021 uno de los actores recibió, a través de su correo electrónico, un mensaje de Google Search Console por el que se le comunicaba la eliminación de la referencia a la mencionada URL o dirección donde se publicaba dicha noticia debido a una solicitud regida por la normativa europea sobre protección de datos. Se aclara que la desindexación solo veía afectados los resultados de las versiones de de búsquedas de Google correspondientes a los países que aplican la normativa europea.

El Tribunal considera que en este caso el único legitimado es Google LLC ya que solamente él puede disponer de los contenidos de dicho buscador por su propietario.

Merece indicar que el Tribunal considera que "*Es necesario destacar que, porque una dirección no aparezca en el motor de búsqueda de Google, no es que no exista, ni que haya sido desaparecida como contenido de Internet. Y el hecho de que se elimine en sus listados a un enlace no significa que se borre el lugar o su contenido de Internet. Todo por el simple hecho de que el motor de búsqueda no aloja al contenido del sitio o página de Internet. En esos casos sólo la URL y su enlace no aparecen en la lista o guía, o no se permite el acceso a través de la página de resultados de búsqueda; mas ello no impide que pueda accederse a la información por otros medios, o a través de otros diferentes motores de búsqueda*".

También se aclara que Google no es el único buscador, por lo que la URL en cuestión puede aparecer en otros listados, y como la información no desaparece de internet, se la puede encontrar teniendo el nombre de la URL. En este sentido, el Tribunal entiende que una cosa es la desindexación (supresión de información sobre un sitio web del listado de un motor de búsqueda) y otra cosa el bloqueo o eliminación de Internet del sitio web (que no se hace por el motor de búsqueda sino a través de una autoridad reguladora). En base a ello el Tribunal considera que el derecho de los actores cuyo amparo procuran no se ha visto afectado en forma trascendente ni de modo manifiestamente ilegítimo.

Es así que el Tribunal expresa que "*Desde el punto de vista que Google no dispone, ni elimina ni bloquea los sitios web. ni sus contenidos, sino que simplemente no los incorpora o restringe su acceso en su listado privado de resultados de búsqueda, no puede decirse que desindexación de una URL suponga una actividad de censura, ni que coarte la libertad de expresión. Es muy cuestionable entonces, al menos dentro de la superficialidad del Amparo y en la óptica expuesta, postular a desindexación como una actividad de restricción de la libertad de expresión o de prensa*".

A ello se agrega que en Uruguay la publicación involucrada puede accederse sin ningún problema bastando ingresar ciertas palabras claves por lo que la desindexación en cuestión no afecta ninguna búsqueda en nuestro país por lo que no surge la conducta manifiestamente ilegítima del demandado.

El Tribunal entiende que, en el caso, de todos modos, el supuesto hecho lesivo ocurrió fuera del Uruguay y no impactó en derechos ejercidos en nuestro país desde el punto de vista que el contenido sigue accesible en la indexación de Google para nosotros.

En términos de ponderación con otros derechos, especialmente con la libertad de expresión, el Tribunal entiende que no se encuentra afectado por que la desindexación de la información involucrada en el motor de búsqueda Google no significa que la URL haya sido bloqueada o eliminada del web, hecho que claramente no sucedió. A eso se agrega que más adelante el Tribunal expresa que los derechos de libertad de expresión y de prensa no son absolutos ni excluyentes de otros, sino que la misma legislación pondera soluciones para la debida armonización de aquellos con otros derechos concurrentes como ser el derecho a la privacidad, la imagen y la dignidad de las personas.

Específicamente sobre el Derecho al Olvido el Tribunal expresa que "*En el Derecho uruguayo es discutible si existe o no el derecho al olvido, no habiendo norma escrita que regule el punto. En el Anteproyecto de Ley de lo que se sancionó como la Ley No. 19.889 existía una previsión (art. 214 del Anteproyecto), pero fue retirada. Podrá sostenerse que en el Uruguay el derecho al olvido no existe, o hasta podría postularse que se encontraría implícito en Derechos Humanos de novísima generación, o que existe un derecho a la memoria y no al olvido; cuestiones sobre las cuales no se discutirá en este pronunciamiento*".

En definitiva, se confirma la sentencia de primera instancia que desestima la acción de amparo impetrada.

Difusión y capacitación de la Unidad

Sitio web

En el año 2021 la Unidad empleó el sitio web con intensidad siendo una de las principales vías de comunicación con la ciudadanía. El sitio web fue una de las herramientas que utilizó la Unidad para transmitir conocimiento e informar de noticias y tendencias nacionales e internacionales en materia de Protección de Datos Personales.

Atención de consultas personalizadas

Como se verá más adelante, la tendencia en materia de consultas continúa refiriendo muchas de ellas a las obligaciones de cumplimiento de los responsables y encargados, la inscripción de bases de datos códigos de conducta, trámite de expedientes, videovigilancia, ejercicio de derechos de acceso, actualización, supresión y rectificación de datos. Se agregan además consultas específicas en el marco de las nuevas obligaciones creadas, con especial énfasis, en los temas de delegados y evaluación de impacto.

Curso en línea de protección de datos

En razón del éxito obtenido en años anteriores, se continuó en el año 2021 con el curso totalmente en línea de Protección de Datos Personales disponible en la plataforma educativa Educantel, con matrícula libre, valorando el trabajo colaborativo y las sinergias generadas por las múltiples ideas plasmadas a través de las participaciones en los distintos foros y el intercambio con los tutores.

Curso de protección de datos personales para funcionarios

En este año se brindaron dos cursos para funcionarios públicos sobre la importancia y contenido del derecho a la protección de datos personales.

La primera edición del curso se dictó entre los días 27 de abril al 14 de mayo. La segunda edición se realizó entre los días 15 de junio y 23 de junio.

En ambos casos, los cursos se desarrollaron con funcionarios públicos de distintas Entidades Públicas.

Curso para delegados de protección de datos personales designados

A los efectos de apoyar en la capacitación de las personas que fueron designados como delegadas tanto en el ámbito público como privado se diseñó y realizó dos ediciones de un curso enfocado para este público.

La primera edición se realizó entre el 12 de abril y el 24 de mayo. La segunda edición se realizó entre los días 26 de julio y 3 de setiembre,

Ambas instancias contaron con amplia asistencia tanto del ámbito público como privado.

Jornada de capacitación para delegados

El 10 de noviembre, bajo la consigna "*Novedades en materia de transferencias internacionales de datos*", se realizó el primer taller para delegados de protección de datos personales con la presencia de 50 representantes de organismos públicos y privados.

Durante la jornada se presentaron las recientes modificaciones en transferencias internacionales, en especial las últimas resoluciones y criterios emitidos por la Unidad. Además, quienes asistieron pudieron intercambiar y evacuar dudas.

Se trata de la primera edición dentro de una serie de capacitaciones enfocadas en la actualización sobre la aplicación y el uso del derecho, dirigidas a delegados de protección de datos personales, considerando su rol dentro de las organizaciones.

Curso de introducción a la protección de datos

Dentro de las tareas esenciales que desarrolla esta Unidad se encuentra el de dar mayor difusión a la existencia tanto del derecho a la protección de datos personales como de la existencia y competencia del órgano de control.

En ese marco, se realiza durante el transcurso del año diversas actividades de difusión para distintos organismos interesados en la temática.

En el año 2021, se brindaron inducciones en materia de protección de datos personales para el SINAE el 8 de febrero, para la Intendencia de Paysandú el 21 de abril, el 7 de setiembre para el Plenario de Municipios, el 10 de agosto para la ANII, el 5 de noviembre para la Intendencia de Tacuarembó y el 6 de diciembre para la Defensoría del Vecino de Montevideo.

Relacionamiento internacional

Participación en grupos de la Asamblea General de la Privacidad

La Unidad participó activamente en calidad de miembro de los Grupos ad hoc creados en el marco de la GPA para analizar los términos y estándares comunes en materia de protección de datos a nivel global, y en el Grupo sobre COVID 19. Atento a la situación de pandemia, las reuniones de ambos grupos se mantuvieron en forma virtual, con una frecuencia mensual o quincenal, según los casos, colaborándose en la redacción de informes, y en la participación de eventos especiales organizados para difundir su trabajo. Los reportes finales del trabajo de los grupos se presentaron en la 43ª. Asamblea Global de Privacidad y se encuentran disponibles en el sitio web de la organización.

Participación en el Consejo Consultivo del Convenio 108 del Consejo de Europa

En función de la situación de pandemia, las actividades del Consejo de Europa se realizaron durante el año 2021 en forma virtual. En la sesión de noviembre de 2020 el coordinador de datos personales, Gonzalo Sosa, asumió el rol de miembro del Bureau del convenio, junto a representantes de Alemania, Georgia, Italia, Rusia, Senegal y Suiza.

Las sesiones plenarias del Convenio 108 se realizaron en forma virtual los días 28 a 30 de junio y 17 a 19 de noviembre, en tanto las reuniones del Bureau –en la misma calidad- se realizaron los días 24 a 26 de marzo, 28 a 30 de setiembre y 20 a 22 de diciembre. La información de la agenda de las reuniones y los reportes pueden encontrarse en el sitio web de protección de datos del Consejo de Europa.

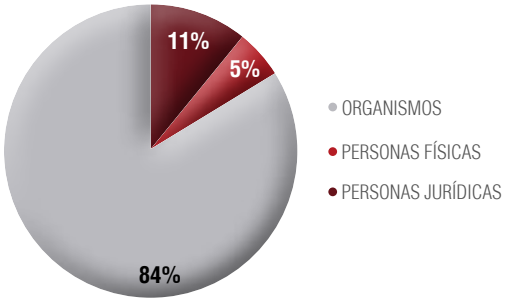
Participación en la Red Iberoamericana de Protección de Datos Personales

La Unidad ha participado, tanto en su rol de miembro de la RIPD, como de su Comité Ejecutivo, en distintos eventos organizados por la Red, como se indicó oportunamente. En el correr del año 2021 la Red ha organizado un conjunto de

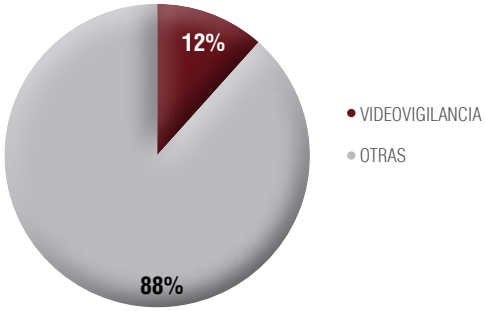
actividades, tanto por parte del Comité citado como del Foro de la Sociedad Civil. El detalle de las actividades de la RIPD en el año 2021 puede encontrarse en la memoria publicada al efecto por la organización.[13]

La URCDP en cifras

En este capítulo se ofrece un panorama general del estado de situación de la protección de datos en Uruguay a partir de



información en clave cuantitativa y gráfica que facilitará el análisis de la actuación de la URCDP.



REGISTRO DE DATOS PERSONALES DE ACUERDO CON EL TIPO DE RESPONSABLE

En las tablas y gráficos siguientes se presentan los resultados del registro online de los formularios ingresados y los aprobados durante el año 2021.

Se continúa observando una mayor tendencia al cumplimiento de las personas jurídicas con respecto a las personas físicas y entidades públicas.

Se presentan, a continuación, los datos de cantidad de bases de datos inscriptas en 2021, discriminadas por tipo de responsables.

Cantidad de bases inscriptas por responsable – Año 2021

Debe tenerse presente que, a partir de la implementación del nuevo sistema, las resoluciones de inscripción de bases de Hojdatos son únicas por cada base presentada, no admitiéndose más inscripción de múltiples bases en una sola resolución.

DIVISIÓN DE LAS BASES DE DATOS SEGÚN LA FINALIDAD DEL TRATAMIENTO - VIDEOVIGLANCIA

El Sistema de Registros permite conocer las distintas finalidades declaradas por los responsables de datos, información imprescindible para determinar la legitimación en el tratamiento.

Actualmente existe un alto porcentaje de bases de datos inscriptas con finalidades de videovigilancia con respecto a la inscripción por el resto de las finalidades declaradas por los responsables.

13 Acceder a la Memoria de Actividades Red Iberoamericana de Protección de Datos. Ejercicio 2021

Porcentaje en cantidad de bases de videovigilancia ingresadas por nuevo Sistema – Año 2021

TRANSFERENCIAS INTERNACIONALES

Las transferencias internacionales de datos se encuentran habilitadas por las normas en materia de Protección de Datos, siempre bajo el cumplimiento de determinados requisitos y la autorización previa de la unidad, salvo contadas excepciones.

Por Resolución del Consejo Ejecutivo N° 23/021, de 8 de junio de 2021, nuestro país ha determinado los países que se consideran adecuados a los efectos de habilitar transferencias internacionales, en concreto, 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.. La resolución se encuentra disponible en el sitio web de la Unidad.

Ello motiva que, en el corriente año 2021, derivado de la diferencia sustancial en el régimen adoptado, no se presente una discriminación de los destinos a los que se realizan transferencias de datos, como en años anteriores.

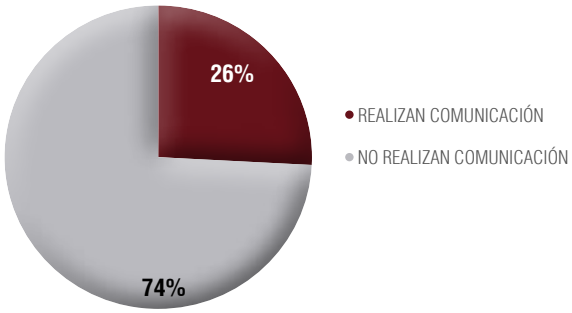
Corresponde sí señalar que se declararon transferencias internacionales durante el año en 80 bases de datos.

TIPO DE INFORMACIÓN

Toda base de datos debe ajustarse a una finalidad determinada, que debe informarse a los titulares de los datos, constituyéndose en uno de los elementos más relevantes al momento de la inscripción. La gran mayoría de las bases de datos integra datos de carácter identificativo y personal.

Parte de esas bases contienen información de “datos especialmente protegidos”, de acuerdo con la normativa nacional vigente.

Los datos especialmente protegidos son:



- Datos sensibles.
- Datos relativos a la salud.
- Datos biométricos.
- Datos personales transferidos internacionalmente.
- Telecomunicaciones.
- Datos de bases de datos con fines de publicidad.
- Datos relativos a la actividad comercial o crediticia.

CESIONES O COMUNICACIONES DE DATOS

El porcentaje de cesiones y comunicaciones de datos que se realizan a partir de las bases de datos que se inscribieron durante 2021 asciende a un 39%, como se observa en la gráfica que sigue, y que es consistente con los datos de años

anteriores.

Comunicaciones de datos realizadas sobre cantidad de bases – Año 2021

CÓDIGOS DE CONDUCTA

Los códigos de conducta refieren a reglas estandarizadas y adoptadas por los responsables de las bases de datos a efectos que el tratamiento de los datos se efectúe de acuerdo con las normas en materia de Protección de Datos. Dichos códigos deben ser inscriptos y aprobados por la unidad.

En el transcurso de 2021 se aprobaron seis códigos de conducta.

DELEGADOS DE PROTECCIÓN DE DATOS

Con la reforma de la Ley de protección de datos N° 18.331, se introdujo a la legislación nacional la figura del delegado de protección de datos. Conforme el artículo 40 de la ley N° 19.670, de 15 de octubre de 2018, y el decreto reglamentario N° 64/020, de 17 de febrero de 2020, las entidades públicas –estatales o no-, y las privadas que traten datos sensibles como negocio principal o grandes volúmenes de datos, deben efectuar la comunicación de delegado de protección de datos.

En el correr del año 2021 se aprobó la comunicación a través del sistema puesto a disposición por la Unidad para tal fin, un total de 67 delegados.

BASES DE DATOS INSCRIPTAS ANTE LA URCDP

Las valoraciones realizadas en oportunidad de analizar cada solicitud de inscripción se describen a continuación:

Valoración notarial: Un escribano público analiza que la empresa cumpla los requisitos formales necesarios para solicitar la inscripción y puede, además, requerir aclaraciones pertinentes en caso de que la información registral obtenida en el Registro de Personas Jurídicas no coincida con lo declarado en el registro.

Valoración jurídica: Un abogado evalúa el cumplimiento de los requerimientos sustanciales previstos por la normativa nacional vigente, solicitando, en caso de eventuales inconsistencias, las aclaraciones que se estimen pertinentes. Este proceso se ha simplificado gracias a la asistencia del sistema informático, que ha sido programado para efectuar validaciones automáticas en buena parte de los campos del nuevo formulario.

Valoración técnica: Si las bases de datos contienen datos especialmente protegidos, un ingeniero de Sistemas analiza las medidas de seguridad propuestas y realiza las recomendaciones de seguridad que considere adecuadas para asegurar la confidencialidad de los datos, pudiendo solicitar aclaraciones si considera que las existentes son insuficientes.

Una vez efectuados los contralores mencionados, el Consejo Ejecutivo de la URCDP dicta una resolución en la que se establece que la base de datos, efectivamente, se inscribió en el Registro de Bases de Datos Personales. En el caso de las bases inscriptas por el nuevo sistema, la resolución es firmada automáticamente con Firma Digital de la unidad.

Durante el año 2021 se inscribieron ante la Unidad por el nuevo sistema un total de 264 bases de datos.

CONSULTAS A LA MESA DE AYUDA DE LA URCDP

La URCDP cuenta con una Mesa de Ayuda que realiza la atención de todas las consultas formuladas en la materia a través de múltiples canales (presencial, telefónica, correo electrónico y formulario de contacto). Todas las consultas formuladas son evacuadas por la asesoría jurídica del Área Derechos Ciudadanos de Agesic.

En atención a la emergencia sanitaria y de las medidas adoptadas por el Gobierno, la mayoría de las consultas fueron evacuadas por vía telefónica o vía correo electrónico y formulario de contacto. Al igual que en años anteriores, durante el año 2021 se recibieron más de 1600 consultas por todas estas vías.

EXPEDIENTES PRESENTADOS POR CONSULTAS Y DENUNCIAS

Acorde al incremento anual del cumplimiento por parte de los responsables de las bases de datos, así como a la difusión de los derechos vinculados con la Protección de los Datos Personales en la ciudadanía, las denuncias y consultas realizadas ante la unidad continúan siendo significativamente menores que las registradas en los primeros años de vigencia de la ley.

Durante 2021, la URCDP recibió 44 consultas, 133 denuncias y 20 solicitudes de informe, respecto de las cuales se formalizó expediente.

RESOLUCIONES QUE IMPONEN SANCIONES

La URCDP tiene competencias en materia de determinación de sanciones otorgadas por el artículo 35 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 este sentido, está habilitada a imponer sanciones a los responsables de las bases de datos, a los encargados del tratamiento de los datos personales y a otros sujetos alcanzados por el régimen de Protección de Datos Personales.

Las sanciones tendrán distintos grados según la gravedad de la acción sancionable y la reiteración o reincidencia.

En 2015 se dictó la Resolución Nº 105/015, que modifica la escala de sanciones a fin de adecuarla a las actuales tendencias sancionatorias considerando la importancia de educar a los responsables y encargados de tratamiento.

Durante 2021 se aplicaron 23 observaciones, 8 apercibimientos y 4 multas y se realizaron 7 intimaciones a responsables para que se adecuaran los procedimientos para el tratamiento de los datos a las disposiciones de la Ley N° 18.331.

RESOLUCIONES Y DICTÁMENES REALIZADOS EN 2020

Durante 2021 se analizaron los expedientes presentados ante la URCDP, además de otros aspectos derivados de la pandemia, y se constató la expedición de 58 resoluciones y 24 dictámenes.

Las personas pueden tener acceso a toda la información a través del sitio web de la URCDP: http://gub.uy/urcdp

CANTIDAD DE INFORMES REALIZADOS

En función de los requerimientos que ha recibido la URCDP, se han elaborado 1328 informes, que incluyen los puntos de vista jurídico, notarial y técnico referidos anteriormente.