MEMORIA 2020

Contenido

ACTIVIDADES ACADÉMICAS DE LA UNIDAD DE PROTECCIÓN DE DATOS PERSONALES

5ta. Semana Nacional de la Protección de Datos Personales

Entre el 26 y 28 de agosto se realizó la 5ta Semana Nacional de Protección de Datos bajo el nombre "Ciencia de datos, marcos éticos y derechos en la reutilización de la información judicial". Las jornadas se realizaron en formato virtual y con gran asistencia de público.

Este evento, que se realiza desde el 2016, tiene el objetivo de promover la difusión y concientización respecto al derecho a la protección de datos personales.

Como es habitual, contó con la presencia de invitados nacionales e internacionales en el marco de las actividades planificadas, y con el apoyo de múltiples organizaciones públicas, privadas y de la sociedad civil.

Las jornadas incluyeron dos paneles diarios. El panel ***"****Reutilización de datos personales: los datos sensibles más allá del principio de finalidad"*, contó con la participación de Jesús Rubí, encargado de área internacional de la Agencia Española de Protección de Datos y Ricardo Roca, presidente de la Comisión Nacional de Ética en Investigación. Ambos expositores reflexionaron sobre las condiciones para la utilización de información sensible fuera de la finalidad para la que fue recolectada. Se tomó como ejemplo el contexto de la pandemia de COVID 19, que pone en evidencia cómo los datos de salud pueden ser utilizados con fines que exceden los intereses particulares y se orientan hacia la defensa de un interés general.

El panel ***"****Responsabilidad proactiva en la práctica: cláusulas contractuales, privacidad desde el diseño y evaluaciones de impacto"* contó con la participación de Juan Agustín Otero, de la Agencia de Acceso a la Información Pública Argentina, y del equipo de la URCDP, integrado por Flavia Baladán, Lylián Massarino, Beatriz Rodríguez, Gonzalo Sosa, Romina Lemmo, quienes realizaron un análisis de las medidas de responsabilidad proactiva que incluye la Ley N° 18.331, con énfasis en la realización de evaluaciones de impacto y los criterios incluidos en la Guía elaborada por ambas autoridades.

En el segundo día de las Jornadas, el tercer panel abordó el tema *"Reutilización de datos personales: marcos éticos y ciencia de datos"*. En este caso participaron Jonathan Mendoza, secretario de Protección de Datos Personales del Instituto Nacional de Acceso a la Información Pública de México y Diego Vallarino, docente de Estrategia, Innovación & Emprendimiento, Posgrado de SI y Gestión de empresas de TI, FCEA, UdelaR. Durante las exposiciones se analizó el marco ético para el tratamiento de datos personales, y cuál es su vínculo con la ciencia de datos; una disciplina que busca extraer conocimiento a partir de datos, de forma sistemática y computacionalmente eficiente.

El cuarto panel fue *"Vulneraciones de seguridad, adopción de medidas, comunicaciones a la autoridad de control y marco jurídico de las actuaciones inspectivas"*. En este caso los integrantes del equipo de la URCDP junto a Ignacio Lagomarsino de Cert.uy, analizaron la información que debe remitirse a la Unidad en

caso de vulneraciones de seguridad, y cuáles son las condiciones, potestades y derechos involucrados en las actuaciones inspectivas.

El último día de las Jornadas, comenzó con el panel ***"Reutilización de datos personales: protección de datos personales, propiedad intelectual y otros derechos"*.** Eduardo Cimato, director de Protección de Datos en la Agencia de Acceso a la Información Pública de Argentina y Beatriz Bugallo, profesora de Derecho Comercial y Propiedad Intelectual, estuvieron a cargo de este panel, en el que analizaron el balance entre los derechos de propiedad intelectual y protección de datos personales. Se consideró además la tensión entre el derecho a la protección de datos y la libertad de expresión, y casos prácticos de interés en materia de propiedad intelectual.

En el cierre, el *"Vías para el ejercicio de derechos consagrados en la Ley N° 18.331 en el marco de las nuevas obligaciones en protección de datos" nuevamente* el equipo de la URCDP analizó los mecanismos para el ejercicio de los derechos consagrados en la ley, considerando en particular los criterios administrativos de la URCDP a la fecha.

Otras actividades académicas de la Unidad

Día de la protección de datos

En el Día Internacional de la Protección de Datos Personales, las autoridades de control de Uruguay y Argentina lanzaron una guía con la finalidad de ayudar a los responsables de tratamiento de datos personales a identificar y minimizar potenciales daños. Esta guía busca constituirse en una referencia obligada para todas aquellas entidades de la región que realicen tratamiento de datos personales.

El documento, elaborado en forma conjunta entre la Agencia de Acceso a la Información Pública de Argentina (AAIP) y la Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay, orienta a las personas que realicen tratamientos de datos para que, desde una etapa temprana, las prácticas y proyectos que puedan afectar los derechos de terceros, sean evaluados y constituidos, de acuerdo a rigurosos criterios de seguridad e integridad.

La guía se inspira en las legislaciones y guías más recientes en la materia, el Reglamento General Europeo de Protección de Datos, el Convenio 108 del Consejo de Europa -convenio suscrito y ratificado por ambos países-, y los Estándares de la Red Iberoamericana de Protección de Datos.

Webinar "Privacidad, protección y tratamiento de datos de salud en el marco del COVID-19: retos y oportunidades"

El 27 de mayo de 2020 el Dr. Felipe Rotondo, Presidente del Consejo Ejecutivo de la Unidad, participó en el webinar organizado por ISOC Cybersecurity SIG, en el que se discutieron distintos aspectos de la protección de datos personales en el marco de la pandemia por COVID-19.

La discusión se centró en particular en las formas de tratamiento de los datos de salud en el marco de situaciones de pandemia y crisis sanitaria, con especial énfasis en los

aspectos de seguridad que deben cumplirse de conformidad con las normas en materia de protección de datos.

Se brindaron distintas perspectivas desde la experiencia y normativa de las autoridades de protección de datos presentes. En particular, se contó con la participación –además de Uruguay- de autoridades de Colombia, Costa Rica, México y Perú.

"Diplomado en Protección de Datos Personales 2020" de la Escuela Libre de Derecho

El 8 de julio, el Dr. Felipe Rotondo, Presidente del Consejo Ejecutivo, participó del acto de clausura virtual del diplomado organizado por la Escuela Libre de Derecho, en el panel titulado "Retos internacionales de la Protección de Datos Personales".

En dicho panel se discutieron los desafíos para la protección de datos desde las perspectivas de los reguladores y de otros actores de la sociedad. Participaron autoridades de Colombia, España, Estados Unidos y miembros de la Academia de Argentina.

Comisión de Relaciones Internacionales de la Asamblea Nacional de Ecuador

El Dr. Felipe Rotondo participó en representación de la URCDP y de la Presidencia de la Red Iberoamericana de Protección de Datos, en el evento organizado el 29 de julio por la Asamblea Nacional de Ecuador, en el marco del tratamiento del proyecto de ley de protección de datos personales del citado país.

El Dr. Rotondo hizo especial referencia al marco de los estándares iberoamericanos y la ley de protección de datos de Uruguay. Estuvo acompañado de autoridades de protección de datos de Chile y México, y de miembros del Poder Legislativo de Brasil.

Conversatorio virtual "El Derecho a la Protección de Datos como Derecho Humano: ¿Corre peligro por las políticas implementadas durante la pandemia?"

El Dr. Felipe Rotondo, Presidente del Consejo Ejecutivo de la Unidad, participó del citado conversatorio, organizado el 5 de agosto por el Instituto Interamericano de Derechos Humanos.

La temática del conversatorio versó sobre la protección de datos personales y su vínculo con las nuevas tecnologías post pandemia.

Participaron, además, autoridades de protección de datos de Colombia y Costa Rica, y miembros de la comunidad académica de la República Argentina.

El Dr. Rotondo hizo referencia al papel del Estado en la ponderación de derechos, en particular el derecho a la salud y a la vida y el derecho a la protección de datos, y a la necesaria transparencia en las decisiones que se adoptan. Además, hizo referencia expresa a las actuaciones y recomendaciones de la Unidad en el marco de la pandemia.

Evento "Extraterritorialidad y la cooperación internacional en Iberoamérica: situación actual y perspectiva futura"

La Unidad participó del evento organizado por la Asociación Latinoamericana de Privacidad (ALAP) el 3 de setiembre de 2020. El evento, en el que el Dr. Gonzalo Sosa,

coordinador de la Unidad, tuvo el propósito de intercambiar opiniones entre autoridades y público en general sobre la importancia de la convergencia en los regímenes de protección de datos personales para la defensa de los derechos de las personas.

Durante la actividad, se discutió además sobre el rol de la Red Iberoamericana de Protección de Datos, los instrumentos de colaboración y los mecanismos para la cooperación en el cumplimiento coactivo de las normas.

El evento organizado por ALAP contó con la participación del secretario de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos de México, Mtro. Jonathan Mendoza, el director de la Agencia de Acceso a la Información Pública de Argentina, Dr. Eduardo Bertoni, y el representante de la Agencia Española de Protección de Datos, Dr. Miguel Ángel Pérez Grande.

Quienes expusieron, dieron sus puntos de vista con respecto al concepto de extraterritorialidad y los desafíos que se presentan a las autoridades de la protección de datos, los mecanismos para asegurar colaboración entre partes, el rol de entidades plurilaterales como la Red Iberoamericana de Protección de Datos Personales.

El Dr. Sosa mencionó la relevancia de las modificaciones realizadas a la Ley N° 18.331, de 11 de agosto de 2008, por la Ley N° 19.670, de 15 de octubre de 2018, en particular las referidas a las notificaciones de vulneraciones de seguridad y la ampliación del ámbito de alcance territorial de la Ley.

Sesión cerrada de la Global Privacy Assembly (GPA)

La GPA realizó su evento anual el 13, 14 y 15 de octubre en forma virtual en el que participaron todos sus miembros, incluida la URCDP, y observadores. Interoperabilidad, Inteligencia Artificial, cooperación entre autoridades, fueron algunos de los temas tratados en el evento de la GPA, además de analizar los trabajos de los distintos grupos de la asamblea.

Durante las jornadas se analizó el progreso de la Dirección Estratégica de la GPA, se presentaron informes sobre la interoperabilidad de las regulaciones de protección de datos en los diversos países, el desarrollo de enfoques innovadores relacionados con la Inteligencia Artificial, la relación de la protección de datos con otros derechos y libertades, la cooperación entre autoridades y la privacidad de los niños, entre otros.

Por otra parte, se analizaron los entregables de los grupos de trabajos creados para finalidades específicas. Se revisó además la ayuda brindada a los gobiernos para afrontar la pandemia del COVID 19 y cuál ha sido el papel del grupo de trabajo creado con ese objetivo.

Por último, se trabajó en la adopción de resoluciones suscritas por los diversos integrantes, como resultado de la visión unificada en materia de privacidad en determinados temas y se definieron las próximas metas de la GPA.

Sesión solemne de reconocimiento a la gestión de Elsa Bibiana Peralta Hernández como comisionada de INFO CDMX

El 10 de noviembre, y con la presencia de autoridades del Sistema Nacional de Transparencia de México, autoridades nacionales del citado país y autoridades internacionales, se realizó un evento de reconocimiento a la Comisionada de del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales de la Ciudad de México.

Se destacó en dicho evento la trayectoria de la comisionada, y su trabajo por la defensa de los derechos de acceso a la información pública y de protección de datos personales, y la igualdad de género.

Participó del evento en representación de la Unidad, el Dr. Felipe Rotondo, en calidad de Presidente del Consejo Ejecutivo.

Semana Nacional de Transparencia 2020 organizada por el Sistema Nacional de Transparencia de México

Entre el 17 y 20 de noviembre se realizó en formato virtual la Semana Nacional de Transparencia 2020 de México, con el tema: Salud Pública y Transparencia. Importancia de la información pública para afrontar crisis sanitarias.

En los diversos paneles organizados se trataron distintos temas asociados a la temática del evento, entre los que se encuentran la transparencia proactiva e información socialmente útil en época de pandemia, información de calidad y veraz durante la crisis sanitaria, rendición de cuentas y contrataciones públicas durante emergencias sanitarias y protección de datos personales en tiempos de COVID-19.

El Dr. Felipe Rotondo, Presidente del Consejo Ejecutivo, participó en el panel denominado “El expediente clínico de la pandemia y su preparación como archivo histórico: sistematización de información, clasificación y protección de datos pesonales”, en el que estuvo acompañado de autoridades públicas y representantes del sector privado de México.

El Dr. Rotondo explicó el sistema uruguayo en la materia, las normas archivísticas existentes y el impacto en la protección de datos personales del tratamiento de datos sensibles.

XVIII Encuentro Iberoamericano de Protección de Datos en modalidad virtual

El 4 de diciembre la Red Iberoamericana de Protección de Datos Personales (RIPD) realizó el XVIII Encuentro Iberoamericano de Protección de Datos en modalidad virtual. La sesión abierta comenzó con las palabras de Dr. Felipe Rotondo, presidente de la Red y del Consejo Ejecutivo de la URCDP, quien dio la bienvenida al encuentro.

Durante el evento se expuso sobre la aplicación de la Ley de Protección de Datos de Brasil y la designación de los miembros de su Autoridad Nacional de Protección de Datos Personales (ANPD). Por su parte, se indicó que Panamá está finalizando la aprobación del Reglamento de desarrollo de su Ley de Protección de Datos de 2019 para hacerla efectiva en marzo de 2021.

Además, se presentaron los informes sobre el estado de las recomendaciones a la Guía de Computación en la Nube cuyo objetivo es orientar el entendimiento del modelo de computación en la nube y de los servicios que se prestan en ese entorno.

También se presentó el proyecto de "Fortalecimiento de la Estrategia de lucha contra la violencia de género contra niñas, adolescentes y mujeres en internet" que se está realizando con la colaboración del Programa Eurosocial+, en el que Uruguay es uno de los países socios.

Por su parte, la Dra. Carmela Troncoso de la Escuela Politécnica Federal de Lausana de Suiza, quien presentó las apps de seguimiento y rastreo de contactos en el contexto de la pandemia.

En la sesión cerrada, se destaca la aprobación del Plan Estratégico de la RIPD para el período 2021-2025, el que fue aprobado por unanimidad.

En el Evento se designó al Dr. Nelson Remolina como nuevo Presidente y se modificó la integración de las vocalías del Comité Ejecutivo de la RIPD, que pasaron a estar a cargo de las autoridades de protección de datos de Argentina, México y Uruguay. Durante la sesión también se aprobó la Declaración Final del Encuentro.

Revista uruguaya de Protección de Datos Personales

Como todos los años desde el 2016, se presentó la nueva edición de la Revista Uruguaya de Protección de Datos, prologada por el Sr. Hebert Paguas, Director Ejecutivo de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) y miembro del Consejo Ejecutivo de la Unidad.

En la sección doctrina se presentaron artículos vinculados a la explicabilidad de la inteligencia artificial, el estado actual de la protección de datos personales, el rol de la autoridad brasileña de protección de datos, el tratamiento de datos de salud, y el impacto en Latinoamérica del Reglamento General de Protección de Datos de la Unión Europea y de los Estándares de la Red Iberoamericana de Protección de Datos. Como en ediciones anteriores, se contó con autores reconocidos a nivel internacional en la materia, en concreto María Angels Barbara Fondevila, Leonardo Cervera Navas, Elsa Bibiana Peralta Hernández, Leonardo Parentoni y Oscar Puccinelli.

La entrevista central se realizó a la directora de la Information Commissioner Office de Reino Unido y Presidenta de la Asamblea Global de Privacidad (GPA por sus siglas en inglés), Elizabeth Denham, quien hizo referencia a los retos de la privacidad en pandemia y al rol de la GPA.

Se incluyó como en números anteriores una selección de dictámenes de interés, en tanto la nota de interés, elaborada por el equipo jurídico de la Unidad, refirió a "La reglamentación de los artículos 37 a 40 de la Ley N° 19.670, de 15 de octubre de 2018".

PRINCIPALES TEMAS DEL AÑO

Aplicación de las normas de Protección de datos Personales y su armonización con otros derechos, deberes y garantías cuando se tratan de datos de salud en casos de emergencia nacional

Por dictamen N° 2/020, de 20 de marzo de 2020, la URCDP indicó que la determinación de las medidas a aplicarse para el tratamiento de los datos en la situación de emergencia nacional sanitaria declarada por el decreto Nº 93/020, de 13 de marzo de 2020, corresponde al Poder Ejecutivo-Ministerio de Salud Pública, sin perjuicio de las competencias legalmente asignadas a otras entidades públicas.

Además, se señaló que el tratamiento de datos de salud directamente relacionado con la situación de emergencia indicada, puede realizarse sin el previo consentimiento informado de los titulares de los datos en el marco de las excepciones previstas en los artículos 9º, 17 y 18 de la Ley Nº 18.331, de 11 de agosto de 2008.

Y se agregó que, en el caso de no requerirse el referido consentimiento por la excepcionalidad mencionada, en el tratamiento y comunicación de los datos deberán observarse, bajo responsabilidad de la entidad actuante, los restantes principios en materia de protección de datos, en especial los de veracidad, finalidad, seguridad de los datos y responsabilidad proactiva (artículos 7, 8, 10 y 12 de la Ley Nº 18.331).

Este Dictamen, y todas las recomendaciones establecidas en el marco de la emergencia sanitaria pueden consultarse en la página web de la Unidad.

Avances en materia de Responsabilidad proactiva

La Unidad, avanzando en la aplicación de las nuevas medidas de responsabilidad proactiva, ha emitido dos resoluciones de interés relacionadas con las condiciones de los delegados.

En primer lugar, la Resolución N° 32/020, de 19 de mayo de 2020, que indica que, a los efectos de la designación de delegados de protección de datos, los responsables, y encargados en su caso, deberán tener en cuenta especialmente su calidad de profesional del área jurídica o poseer conocimientos en Derecho, con énfasis en derechos humanos, y conocimientos sobre regulación en materia de protección de datos personales. Esta norma indica que podrá acreditarse mediante cursos o actividades brindadas por la URCDP u otras entidades nacionales e internacionales, valorándose especialmente la realización de cursos vinculados a responsabilidad proactiva y tratamiento de categorías especiales de datos. Asimismo, se establece que se tendrá en cuenta la experiencia previa en el ámbito de la protección de datos.

Esta Resolución indica además que, para el tratamiento de datos sensibles, especialmente protegidos u otros que se definan oportunamente, el delegado deberá poseer conocimientos o experiencia en el área de negocio correspondiente, y en aspectos vinculados a la seguridad de la información y gestión de herramientas informáticas. Además, se indica que en el caso de delegados personas jurídicas, deberá comunicarse a la Unidad Reguladora y de Control de Datos Personales cómo está integrado su órgano de administración, así como los datos de sus integrantes y de la persona o personas físicas que se nominen para realizar la tarea, acreditándose las condiciones de estas personas físicas. Las comunicaciones de designación de delegados que cumplan con las condiciones señaladas, serán consideradas por la Unidad ante cada gestión, sin perjuicio de las revisiones periódicas y solicitudes de actualizaciones a los delegados designados que se determinen.

Por su parte, la Resolución N° 44/020, de 21 de julio de 2020, establece que los conocimientos de los delegados de protección de datos deberán ser valorados por los responsables y encargados, considerando los criterios indicados por este Consejo Ejecutivo por Resolución N° 32/020, de 19 de mayo de 2020, y acreditarse al momento de la comunicación.

Señala que el énfasis en derechos humanos del conocimiento en Derecho mencionado en la Resolución N° 32/020, de 19 de mayo de 2020, refiere al necesario para contextualizar el derecho a la protección de datos en sus relaciones con otros derechos fundamentales, especialmente para delegados que no pertenezcan al ámbito jurídico. Indica que, si los responsables y encargados designan equipos integrados por varias personas para el cumplimiento de la función de delegado de protección de datos, se deberá especificar una de ellas para actuar como nexo con la Unidad (artículo 40 literal D de la Ley N° 19.670, de 15 de octubre de 2018).

Datos biométricos

La Resolución N° 30/020, de 12 de mayo de 2020, de esta Unidad, en el marco de la responsabilidad proactiva establece que todo responsable, y encargado en su caso, que realice tratamiento de datos biométricos, deberán efectuar una evaluación de impacto a la protección de datos personales, en las condiciones y plazos previstos en el artículo 7° del Decreto N° 64/020, de 20 de febrero de 2020. Ello sin perjuicio de las medidas que corresponda adoptar de conformidad con lo establecido en el artículo 5° del mencionado decreto.

Buenas prácticas para formularios digitales

La Unidad Reguladora y de Control de Datos Personales generó una serie de buenas prácticas para que los organismos públicos apliquen a la hora de generar formularios web que recogen datos personales. En la actualidad, la generación de bases de datos de calidad es fundamental para el funcionamiento de las organizaciones. Esto permite mejorar la calidad del relacionamiento entre las personas y la organización, así como facilitar sus procesos internos, mejorando la eficiencia de la misma.

En muchas ocasiones, estas bases de datos están alimentadas por información que se recoge en formularios digitales. Por esto, la URCDP reunió diez buenas prácticas orientadas especialmente a las organizaciones de carácter público, para que puedan crear y distribuir formularios web que recojan datos personales.

El documento incluye recomendaciones sobre la elección de los sistemas, los mecanismos de autenticación, la gestión de los datos recolectados, su conservación y evaluación de impacto. Además, se hace referencia a la importancia de la participación del Delegado de Protección de Datos personales en la generación de los formularios, así como la inclusión de cláusulas que incluyan las condiciones del tratamiento de los datos, para que las personas puedan ejercer sus derechos en el mundo digital.

Sobre información personal y acceso a la información pública

Por Dictamen N° 7/020, se contesta la consulta presentada por el Ministerio de Defensa Nacional solicitando el asesoramiento de la Unidad en relación a si los haberes de retiro y pensiones que paga el Servicio de Retiros y Pensiones de las Fuerzas Armadas, deben considerarse información de carácter pública o ser tratados como datos sensibles. En este caso se indica que no existe impedimento desde el punto de vista de la protección de datos personales para publicar la información relativa a los haberes de personal militar superior, en las mismas condiciones que la del personal militar inferior.

Asimismo, mediante Dictamen N° 8/020, de 2 de junio de 2020, se dictamina acerca de la consulta presentada por la Dirección de Asuntos Constitucionales, Legales y Registrales del Ministerio de Educación y Cultura sobre una solicitud de acceso a la información pública requiriendo datos personales de Asociaciones Civiles y Fundaciones obtenidos en oportunidad de la realización del Censo Nacional.

En este dictamen se establece que corresponde entregar la información indicada en el artículo 9° literal C de la Ley N° 18.331, de 11 de agosto de 2008, respecto de las Asociaciones Civiles y Fundaciones, con excepción de la identidad de las personas a cargo en el caso de Clubes Cannábicos, en función de lo ya dictaminado por este Consejo Ejecutivo por Dictamen N° 3/017, de 14 de junio de 2017, y de aquellas que provengan de otras normas a consideración del consultante, lo que deberá justificarse.

Mediante Dictamen N° 12/020 de esta Unidad se analiza la consulta remitida por la Dirección General del Instituto del Niño y Adolescente del Uruguay, acerca de si es posible incluir nombre, además de documento de identidad, en las actas de las distintas etapas de los concursos que se notifican exclusivamente por la Web, así como en las elecciones de los integrantes de Tribunales internos que realiza la Sección de Calificaciones y Ascensos de la División Gestión y Desarrollo Humano del Instituto.

Según lo dispuesto en el artículo 4 literal D) de la Ley N° 18.331, de 11 de agosto de 2008, los datos identificatorios mencionados tienen el carácter de dato personal. El literal B) de dicho artículo define el concepto de comunicación de datos como *"toda revelación de datos realizada a una persona distinta del titular de los datos."***.** Que el artículo 17 de la Ley Nº 18.331 del 11 de agosto de 2008 incluye entre los supuestos habilitantes de la comunicación los previstos en el artículo 9° (lit. B), a los datos que provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación (apartado a). Se expresa que el artículo 9 BIS considera como públicas o accesibles al público, determinadas fuentes, entre las cuales se encuentran: *"Todo otro registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos puedan ser consultados, difundidos o utilizados por parte de terceros. En caso contrario, se podrá hacer uso del registro o publicación mediante técnicas de disociación u ocultamiento de datos personales.*" En función de lo indicado, aun cuando el dato personal no reviste la calidad de público y su comunicación debe ceñirse a los principios establecidos en la

ley, en este caso se aplican las excepciones indicadas, por lo que es posible publicar las etapas de los concursos en la Web con los datos indicados en la consulta. Ello sin perjuicio de la clasificación o calificación que se realice por parte del organismo, de la información contenida en los expedientes de concurso. Se deben tener presentes criterios de desindexación para evitar conflictos con la protección de los datos personales, a cuyos efectos corresponde tener en cuenta la Resolución de este Consejo N° 1040/2012, de 20 de diciembre de 2012

Intercambio de información en el ámbito educativo

Por Dictamen N° 18/020, de 8 de diciembre, se dictamina sobre la consulta presentada por la Unidad de Análisis e Intervención de la Dirección de Derechos Humanos de la Administración Nacional de Educación Pública (ANEP), en relación con la última etapa del intercambio intersectorial Educación – Salud/Salud Educación establecida en la Hoja de Ruta del proyecto INDI ("Inventario de Desarrollo Infantil").

En el caso, la comunicación de datos ya se analizó y se concluyó que se encuentra debidamente habilitada por la existencia de interés legítimo del emisor y del destinatario, y que en cuanto al consentimiento se encuentra habilitada por el literal b) del artículo 17 de la citada norma (funciones propias de los organismos). En cuanto a los medios para el envío de esa información a maestros y directores, cabe indicar que la información puede ser remitida a los directores de escuela por medio de la plataforma Gurí, por ser la forma más segura en virtud de que se trata de un software de uso institucional que cuenta con suficientes medidas de seguridad. Si ello no fuera posible, ANEP deberá identificar un medio alternativo que ofrezca similares garantías de seguridad de la información, máxime teniendo presente que se está ante datos de salud de menores de edad. En ese sentido, la utilización de pendrives no es una medida adecuada para comunicar la información.

En cuanto a los requisitos para la comunicación, solamente se deben comunicar los datos estrictamente necesarios, y contar con roles debidamente identificados y limitados a aquellos que deban acceder para el cumplimiento de sus cometidos, así como informar en forma debida a los representantes legales de los menores de edad. La planilla remitida y el contenido establecido, considerando los objetivos del proyecto, se consideran correcta.

Por último, conforme con el art. 12 de la Ley N° 18.331, en la redacción dada por el art. 39 de la Ley N° 19.670, y los artículos 6 y 7 del Decreto 64/020, cuando el tratamiento de datos tenga como objeto el tratamiento de datos de poblaciones de especial vulnerabilidad, como ser menores de edad, corresponde la realización de una evaluación de impacto en la protección de datos, para lo que se cuenta con un plazo de un año a partir de la publicación del citado decreto en el Diario Oficial.

RECOMENDACIONES DE LA URCDP EN EL MARCO DEL CORONOVIRUS COVID 19

En virtud de la emergencia sanitaria nacional declarada por el Ministerio de Salud Pública como consecuencia del Coronavirus COVID 19, esta Unidad se abocó al análisis del tratamiento de datos personales en esta especial situación.

En ese marco, esta Unidad realizó recomendaciones diversas y emitió resoluciones ante las distintas situaciones que esta situación genera en la sociedad, las que se presentan a continuación:

Dictamen N° 2/020, de 20 de marzo de 2020, referido a la aplicación de las normas de protección de datos personales y su armonización con otros derechos, deberes y garantías, cuando se tratan datos de salud en casos de emergencia nacional.

VISTO:

La emergencia nacional sanitaria declarada por decreto Nº 93/020, de 13 de marzo de 2020, como consecuencia de la pandemia originada por el virus COVID-19.

CONSIDERANDO:

I. Que en virtud de la situación excepcional referida, resulta pertinente pronunciarse respecto a la aplicación de las normas de protección de datos personales y su armonización con otros derechos, deberes y garantías, cuando se tratan datos de salud.

II. Que la Constitución en su art. 7 prevé para los habitantes la protección en el goce de sus derechos fundamentales y la privación de aquella mediante ley que se estableciere por razones de interés general. El art. 44, por su parte, establece el deber de todos los habitantes de cuidar su salud y asistirse en caso de enfermedad.

III. Que el derecho a la protección de datos personales es inherente a la personalidad humana por lo que está comprendido en el art. 72 de la Constitución como lo explicita el art. 1º de la Ley Nº 18.331 de 11 de agosto de 2008.

IV. Que el art. 4° "E" de la citada Ley refiere a datos sensibles, entre otros los que revelen informaciones referentes a la salud de las personas; su decreto reglamentario Nº 414/009 de 31 de agosto de 2009, art. 4º "D" establece que tales informaciones se relacionan con la salud pasada, presente y futura, física o mental de una persona.

V. Que el tratamiento de datos personales en general requiere del cumplimiento de principios mencionados por la ley Nº 18.331, art. 5º a 12, y el aseguramiento del ejercicio de derechos consagrados en los art. 13 a 17. Los relativos a la salud integran una categoría especial con un nivel adicional de protección, lo que se aprecia en los arts. 18 y 19 de la referida Ley y normativa concordante (a modo de ejemplo Ley Nº 18.335, de 15 de agosto de 2008 y art. 194 de la Ley Nº 19.670, de 15 de octubre de 2008).

VI. Que la regla del previo consentimiento por parte del titular de los datos tiene una excepción a los efectos de la comunicación cuando esta sea necesaria por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de los titulares mediante mecanismos de disociación adecuados cuando ello sea pertinente, según lo establece el art. 17 de la ley Nº 18.331 en el texto dado por el art. 153 de la ley N.º 18.719 de 27 de diciembre de 2010. De similar manera, el art. 18 prevé la recolección y tratamiento de datos sensibles si median razones de interés

general autorizadas por ley o cuando el organismo solicitante tenga mandato legal al efecto.

VII. Que la determinación de la excepcionalidad de las medidas a adoptarse en situaciones de emergencia como la referida en el "Visto" a nivel nacional corresponde al Ministerio de Salud Pública en atención a lo dispuesto en la Ley Nº 9.202 de 12 de enero de 1934, art. 1º y 2º.

ATENTO: A lo expuesto,

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

DICTAMINA:

1°. La determinación de las medidas a aplicarse para el tratamiento de los datos en la situación de emergencia nacional sanitaria declarada por el decreto Nº 93/020, de 13 de marzo de 2020, corresponde al Poder Ejecutivo-Ministerio de Salud Pública, sin perjuicio de las competencias legalmente asignadas a otras entidades públicas.

2°. El tratamiento de datos de salud directamente relacionado con la situación de emergencia indicada en el numeral anterior, puede realizarse sin el previo consentimiento informado de los titulares de los datos en el marco de las excepciones previstas en los artículos 9º, 17 y 18 de la Ley Nº 18.331, de 11 de agosto de 2008.

3° Aún en el caso de no requerirse el referido consentimiento por la excepcionalidad mencionada, en el tratamiento y comunicación de los datos deberán observarse, bajo responsabilidad de la entidad actuante, los restantes principios en materia de protección de datos, en especial los de veracidad, finalidad, seguridad de los datos y responsabilidad proactiva (artículos 7, 8, 10 y 12 de la Ley Nº 18.331).

4°. Publíquese y oportunamente archívese.

Recomendaciones para el tratamiento de datos personales ante la situación de emergencia sanitaria nacional

La emergencia sanitaria declarada por el Decreto N° 93/020, de 13 de marzo de 2020, y derivada de la pandemia del coronavirus COVID-19, ha generado en múltiples actores la necesidad de emplear información personal para atender todo lo relacionado con la enfermedad y, especialmente, mitigar sus efectos adversos sobre las personas y la sociedad. En ese marco, corresponde recordar que el empleo de información personal se encuentra alcanzado por normas que reconocen el derecho a la Protección de Datos Personales como un derecho fundamental. Por ello, es imperativo realizar un uso responsable de dicha información, procurando, hoy más que nunca, alcanzar equilibrios con otros derechos. En ese sentido, la Unidad Reguladora y de Control de Datos Personales realiza las siguientes recomendaciones a ser tenidas en cuenta por personas y entidades públicas o privadas que desarrollen un tratamiento de datos personales asociados al coronavirus COVID-19.

1) Los datos de salud son datos sensibles y su tratamiento requiere como principio el cumplimiento de requisitos especiales, en particular, contar con el consentimiento previo, expreso, informado, específico, inequívoco y escrito de los titulares de los datos.

Adicionalmente, corresponde tomar medidas de responsabilidad proactiva, como las evaluaciones de impacto previas.

2) Se debe tener en cuenta que los sujetos legitimados para el tratamiento de datos de salud son los establecimientos sanitarios públicos o privados, los profesionales vinculados a las ciencias de la salud y el Ministerio de Salud Pública en cumplimiento de los cometidos que le asigna la Ley.

3) Se debe considerar que fuera de los casos previstos en el numeral anterior, el tratamiento y la comunicación de datos de salud deben hacerse con el consentimiento del titular en las condiciones antes mencionadas o en el marco de alguna de las excepciones taxativamente establecidas en la ley a saber, razones de interés general autorizadas por ley, cuando el organismo solicitante tenga mandato legal para hacerlo, o para finalidades estadísticas o científicas, en este último caso disociado de sus titulares.

"Disociar" implica un procedimiento por el cual la información no puede vincularse a persona determinada o determinable, por lo que debe descartarse cualquier tratamiento con información que pueda volver a vincularse con una persona, salvo cuando la ley expresamente lo permita.

4) El consentimiento escrito no requiere que la persona se encuentre presente, pero se deben adoptar medidas que garanticen su debida autenticación y la conformidad con toda la información necesaria para entender los fines y consecuencias de dicha conformidad, lo que debe ser debidamente documentado.

5) En ningún caso los responsables del tratamiento de datos quedan eximidos del cumplimiento de los demás principios generales de la Protección de Datos Personales. Así, los datos recolectados deben ser los mínimos necesarios para el cumplimiento de la finalidad informada y no emplearse para fines distintos o incompatibles con aquellos que motivaron su recolección. Deben adoptarse medidas para garantizar la seguridad y confidencialidad de los datos y otras medidas técnicas y organizativas comprobables para garantizar un tratamiento acorde a la legislación vigente. Se desaconseja el uso de formularios o sistemas en línea que no brinden las debidas garantías de seguridad o confidencialidad en el tratamiento de los datos personales.

6) Es fundamental informar al personal del responsable de los datos recabados sobre el cuidado de la información personal y las consecuencias penales asociadas a la revelación de dicha información. Resulta también conveniente estipular las condiciones para el tratamiento de la información en contratos que se suscriban con los encargados de tratamiento.

7) El tratamiento adecuado de los datos personales requiere asegurar el cumplimiento de los derechos de los titulares de los datos, en la forma y en los plazos que prevé la legislación vigente. Debe cumplirse con el derecho de información previamente a la recolección, con el derecho a la impugnación de valoraciones personales ante el requerimiento del titular afectado y con los derechos de acceso, rectificación, actualización, inclusión y supresión en el plazo de 5 días hábiles desde su ejercicio.

8) No pueden realizarse transferencias internacionales a países no adecuados sin la autorización previa de la URCDP. El uso de sistemas o servicios en la nube –incluso de

almacenamiento- puede constituir una transferencia internacional si los servidores se encuentran en el exterior.

9) Son obligaciones legales formales la inscripción de todas las bases de datos de todo responsable y la designación del delegado de Protección de Datos en los casos en que la ley lo establece (entidades públicas y privadas que traten grandes volúmenes de datos y datos sensibles como negocio principal).

Resolución N° 35/020, de 9 de junio de 2020, que resuelve sobre los lineamientos para la utilización de sistemas de rastreo de contacto ("contact tracing") mediante aplicaciones móviles.

VISTO: La pertinencia de brindar lineamientos para la utilización de sistemas de rastreo de contacto ("contact tracing") mediante aplicaciones móviles con respeto de los principios de la protección de datos personales.

CONSIDERANDO:

I) Que se tienen en cuenta las siguientes circunstancias:

a) Distintas autoridades sanitarias a nivel mundial han planteado la conveniencia de desarrollar aplicaciones que incluyan sistemas para monitorear los movimientos de las personas según áreas geográficas y determinar vínculos de proximidad entre personas infectadas y personas sanas. En el primer caso, el monitoreo permitiría realizar predicciones y controlar la expansión; en el segundo, informar a potenciales infectados para que adopten las medidas necesarias para asegurar su salud.

b) En relación a las especificaciones técnicas vinculadas al almacenamiento de la información de contacto, se distinguen actualmente sistemas con almacenamiento centralizado y los que descentralizan su operación, almacenando la información de contacto en los propios dispositivos de los usuarios.

c) El informe del Comité Europeo de Protección de Datos N° 4/2020 señala que los datos de ubicación necesarios para el funcionamiento de los sistemas de rastreo de contactos pueden provenir de proveedores de servicios de comunicaciones electrónicas o de aplicaciones que requieren el uso de dichos datos, recolectados por proveedores de servicios de la sociedad de la información.

d) Las aplicaciones móviles ya desarrolladas cuentan con otras funcionalidades vinculadas a la provisión de información general sobre la pandemia, el auto-monitoreo del estado de salud, y mecanismos de telemedicina, entre otras.

e) Adicionalmente, dichas aplicaciones solicitan información personal de naturaleza sensible, por lo que se impone su uso responsable, adecuado y ponderado, atento a los riesgos que importan para la privacidad de las personas.

f) Distintas entidades a nivel global (entre ellas la Red Iberoamericana de Protección de Datos, la "Global Privacy Assembly" y el Consejo de Europa) han elaborado documentos de buenas prácticas sobre la protección de la privacidad durante el

transcurso de la pandemia y la Organización Mundial de la Salud emitió recientemente una Guía con consideraciones éticas para el uso de la tecnología de rastreo de contacto en el marco de la pandemia por COVID-19.

g) Esta Unidad se ha pronunciado con respecto al tratamiento de datos en la situación de la emergencia nacional sanitaria a través del Dictamen N° 2/020, de 20 de marzo de 2020, brindando directivas específicas en la materia.

II) Que la aplicación de sistemas de rastreo de contacto y su inclusión en otras aplicaciones en desarrollo requiere un análisis de ponderación entre el derecho y el deber a la salud y el derecho a la protección de datos personales –incluido en el artículo 72 de la Constitución Nacional como se explicita en el artículo 1° de la Ley N° 18.331, de 11 de agosto de 2008-.

III) Que, la comunicación de datos personales por razones sanitarias o de emergencia corresponde se efectúe, de principio en forma disociada, habilitando la identificación del titular del dato en circunstancias particulares (artículo 17 literal C); fuera de ese caso, se requerirá el consentimiento del titular del dato (artículo 9° de la Ley citada). Adicionalmente y en lo que respecta al empleo de datos de contacto, si estos son obtenidos de operadores de telecomunicaciones es aplicable el artículo 20 de esa Ley, y 6° del Decreto N° 64/020, de 17 de febrero de 2020, por tratarse de datos especialmente protegidos.

IV) Que el monitoreo a gran escala de los contactos de las personas no posee una base legal que lo habilite sino que esta radica en el previo consentimiento informado, el que podrá recabarse por medios electrónicos. El tratamiento de estos datos podrá realizarse exclusivamente por el período de duración de la emergencia sanitaria, en el marco de una política de mitigación de la pandemia, y bajo el estricto control y responsabilidad de la autoridad sanitaria, en cumplimiento de un mandato legal de conformidad con la ley Nº 18.331, art. 18° de la Ley N° 18.331 y Ley N° 9.202, de 12 de enero de 1934.

V) Que en todo caso deben tenerse presentes los principios de protección de datos personales que explicita la ley Nº 18.331, en especial los principios de veracidad (artículo 7°), finalidad (artículo 8°), consentimiento informado (artículo 9°) seguridad de los datos (artículo 10), y responsabilidad proactiva (artículo 12). También garantizarse el ejercicio de los derechos de los titulares de los datos (artículos 13 a 17, y cumplir las medidas previstas en el Decreto N° 64/020.

ATENTO: a lo expuesto y a normativa concordante,

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

RESUELVE:

1) Efectuar las siguientes consideraciones respecto al uso de sistemas de rastreo de contacto en el ámbito de la emergencia nacional sanitaria, a efectos de la adecuada protección de los datos personales:

I. En cuanto a los sistemas de rastreo de contactos, aconsejar los que implican un almacenamiento descentralizado de los datos por resultar menos invasivos para la privacidad de las personas.

II. Señalar la pertinencia de realizar en forma previa una evaluación de impacto en la protección de datos; la inscripción de la base generada en caso de contener datos personales, o en su caso, actualizar la preexistente; y la suscripción de acuerdos que garanticen el cumplimiento de la normativa en caso en que se aplique sistemas provistos por terceros así como analizar y evaluar especialmente los aspectos técnicos vinculados con seguridad, considerando especialmente los lineamientos del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CertUy) de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.
III. En caso que el rastreo de contactos se adicione como funcionalidad a aplicaciones preexistentes que recolecten otro tipo de información, deberán extremarse las medidas de seguridad, atendiéndose otras alternativas en el marco de la necesaria evaluación de impacto a la protección de datos.

IV. Corresponde asegurarse la obtención del consentimiento previo y expreso de los usuarios mediante la descarga y aceptación de términos de la aplicación, o en caso de que se agregue como funcionalidad a aplicaciones pre-existentes, de las nuevas funcionalidades y actualizaciones que se propongan incluir en el sistema.

V. Deberá establecerse una adecuada granularidad del consentimiento ante distintas acciones propuestas a los titulares de los datos, y prever la posibilidad que éstos puedan revocar su consentimiento para el uso del rastreo de contacto, aún sin tener que eliminar la aplicación.

VI. Procede asegurarse que el sistema sólo pueda ser aplicado por el Ministerio de Salud Pública en el marco de la emergencia sanitaria en su calidad de responsable de tratamiento de datos, y con fines de alertar a potenciales contagiados, del contacto con una persona positiva por COVID-19. Adicionalmente, no debe emplearse para realizar un monitoreo individual de los usuarios.

VII. La información debe almacenarse en centros seguros y en territorio nacional. En casos debidamente justificados de transferencia internacional, deberá solicitarse la autorización a esta Unidad, salvo que se transfiera a territorios adecuados. Los respaldos deberán cumplir con las recomendaciones indicadas en el presente y deberán ser eliminados en las mismas condiciones que las bases originales.

VIII. En caso de conservarse información en forma centralizada –fuera de los dispositivos de los usuarios- se debe contar con los mecanismos de seguridad pertinentes para evitar incidentes y ser eliminada una vez cumplida la función para la cual fue recolectada.

IX. Como corolario de lo anterior, y en caso de que se agregue el rastreo de contacto a una aplicación preexistente, mantenerse independiente la información vinculada a éste de la que resulte de otras funcionalidades de la aplicación.

X. No deberá proporcionarse información personal de casos positivos a potenciales contagiados por la enfermedad; tal información sólo puede remitirse al Ministerio de Salud Pública con el consentimiento expreso del titular del dato y a efectos del seguimiento de su situación de salud. Cuando el rastreo de contactos se adicione a una aplicación preexistente, la comunicación de confirmación de un caso positivo debe efectuarse con el consentimiento expreso del titular del dato.

XI. Deberá ponerse a disposición de los interesados las especificaciones de la aplicación a efectos de garantizar un tratamiento transparente de los datos y un eventual consentimiento informado. En particular, especificarse la forma de habilitar o deshabilitar el rastreo de contactos y la información sobre el uso de bluetooth; si ésta se adiciona a una aplicación preexistente, deberá aclararse expresamente y en forma separada las condiciones de tratamiento de otras funcionalidades de la aplicación.

XII. Procede informarse expresamente a los titulares de los datos sobre situaciones de potencial contagio y los parámetros de tiempo y distancia, así como eventuales modificaciones, en el marco de la necesaria y permanente transparencia.

XIII. Deberá minimizarse la recolección de información, en especial cuando refiere a informaciones de terceros; en su caso, estas sólo podrán remitirse al Ministerio de Salud Pública para su gestión conforme los protocolos que se elaboren al respecto, manteniéndose separadas de la información derivada del rastreo de contactos. También eliminarse toda la información finalizada la emergencia sanitaria, salvo que sea debidamente anonimizada y su conservación autorizada por la Unidad. La información recolectada debe ser periódicamente revisada en función de los objetivos específicos considerando un criterio de minimización de los datos.

2) PUBLÍQUESE.

Recomendaciones para el tratamiento de datos personales en el marco del teletrabajo

El teletrabajo es una forma de trabajo que se realiza en una ubicación alejada de una oficina central o instalaciones de producción que separa a la persona del contacto personal con colegas que estén en esa oficina Esta modalidad, ha vuelto comunes las herramientas que permiten las reuniones a distancia, su grabación y almacenamiento, el intercambio de archivos, la utilización de la nube, con un incremento exponencial en el tratamiento de información personal a través de internet.

El empleo de información personal se ampara en la normativa que reconoce a la protección de datos personales como un derecho fundamental. En esta línea, la Unidad Reguladora y de Control de Datos Personales pone a disposición las siguientes recomendaciones dirigidas a personas y entidades públicas o privadas que estén desarrollando o pretendan desarrollar herramientas de teletrabajo:

1. Definir previamente las herramientas y los dispositivos a utilizar, así como los tipos de archivos que se necesiten intercambiar.
2. Generar políticas internas que tengan como objetivo identificar diferentes perfiles, con sus correspondientes niveles de acceso.

3. Elaborar guías funcionales sobre la forma de tratamiento de datos personales, especialmente cuando se utilicen dispositivos personales o conexiones a Internet domésticas.
4. Determinar los medios para informar o capacitar sobre los alcances de las herramientas empleadas y las posibles amenazas a los datos personales, además de prever un proceso interno para comunicar eventuales incidentes de seguridad que los afecten.
5. En el caso que se requieran servicios de terceros, se recomienda elaborar contratos que determinen claramente las obligaciones y derechos de las partes. Si el contratado accede a información personal asumirá la calidad de encargado de tratamiento de datos.
6. Determinar los mecanismos y plazos para el almacenamiento de la información transmitida (video, voz, archivos, etc.), y en particular su ubicación, con el objetivo de determinar si se trata de una transferencia internacional, que requiera autorización de la URCDP.
7. Configurar técnicamente los equipos informáticos para asegurar la privacidad de las comunicaciones (instalar antivirus, política de contraseñas, accesos remotos a recursos de la organización, etc.).
8. Informar a quienes trabajan en la organización si se van a utilizar sistemas de monitoreo, y qué tratamiento se va a dar a la información obtenida.
9. Contar con los medios necesarios para hacer efectivos los derechos que prevé la legislación (Ley Nº 18.331 y modificativas) para la protección de datos personales (acceso, rectificación, supresión, actualización, impugnación de valoraciones personales).
10. En caso de tratamiento de datos personales de más de 35.000 personas, se recomienda realizar una evaluación de impacto en la protección de datos.
11. Tener en cuenta las Recomendaciones técnicas para implementar el teletrabajo puestas a disposición por Agesic.

Recomendaciones para el control de temperatura ante la situación de emergencia sanitaria nacional

La emergencia sanitaria declarada por el Decreto N° 93/020, de 13 de marzo de 2020, y derivada de la pandemia del coronavirus (COVID-19), ha generado en múltiples actores la necesidad de emplear diversas técnicas para salvaguardar la seguridad y salud de las personas, y de la sociedad en general.

En ese marco, corresponde recordar que el empleo de información personal se encuentra alcanzado por normas que reconocen el derecho a la Protección de Datos Personales como un derecho fundamental. Por ello, es imperativo realizar un uso responsable de dicha información, procurando, hoy más que nunca, alcanzar equilibrios con otros derechos. En los últimos meses, se ha observado la utilización de distintos dispositivos para corroborar la temperatura de las personas previo al ingreso a lugares de trabajo, espacios cerrados privados y oficinas públicas, en el entendido que una temperatura elevada se asocia con la enfermedad producida por el coronavirus (COVID-19).

A fin de clarificar los alcances de dichas medidas con respecto a la protección de datos personales, la Unidad Reguladora y de Control de Datos Personales realiza las siguientes recomendaciones a ser tenidas en cuenta por personas y entidades públicas o privadas que empleen mecanismos de control de temperatura:

1. Dato personal es toda información que permite identificar o hacer identificable a una persona, por lo que la temperatura en sí misma no constituye un dato personal. Su asociación a una persona lo transforma en un dato personal de naturaleza sensible, por referir a la salud, y requiere medidas de seguridad especiales.

2. La asociación del dato a la persona puede provenir no sólo de un registro manual de identidad (nombre, apellido, y demás datos identificatorios), sino también de otros mecanismos como la captación de su imagen.

3. El dato temperatura solo puede utilizarse con la finalidad de garantizar la seguridad y salud de las personas. Si el dato se registra, se deberá informar el tiempo de conservación de esa información, y justificar debidamente las razones para ello.

4. En los accesos de personas a establecimientos públicos y/o privados corresponde considerar la seguridad y salud de las personas que trabajan y circulan en ellos, en cuyo caso podrán emplearse mecanismos de control de temperatura siempre que no se almacene información personal de los titulares de los datos.

5. El control de temperatura de empleados por parte de los empleadores puede realizarse con el fin de garantizar su seguridad y salud, mediante protocolos acordados con las áreas de recursos humanos para proteger la privacidad de los titulares de los datos, y siguiendo las recomendaciones del Ministerio de Trabajo y Seguridad Social.

6. El control de temperatura en ámbitos donde no está presente el riesgo de la seguridad o salud de las personas, sólo se podrá realizar garantizando el anonimato de la persona, o mediante normas jurídicas que lo habiliten expresamente.

7. En todos los casos, la adopción de medidas de control de temperatura puede realizarse luego de consideradas otras menos intrusivas, que generen el mismo resultado.

8. Los equipos de temperatura que se utilicen deben ser fehacientes en su aplicación y el personal que los utilice debe contar con la capacitación necesaria.

9. En caso de utilizarse cámaras térmicas digitales (que adquieren y procesan información de temperatura digitalmente además de la imagen de la persona), cualquier dato obtenido debe considerarse como tratamiento automatizado de datos personales.

10. Se debe garantizar el derecho a la información a todas las personas en cuanto a la forma de utilización de este tipo de dispositivos y los procedimientos a aplicar cuando se supere la temperatura establecida.

11. La medición de temperatura solamente se debe realizar en tanto persista la emergencia sanitaria declarada, y debe finalizar una vez cesada dicha emergencia.

12. Todas las medidas que se adopten al respecto deberán tomar en cuenta los criterios y recomendaciones brindados por el Ministerio de Salud Pública.

AVANCES NORMATIVOS

Decreto 64/020, de 17 de febrero de 2020

La Ley Nº 19.670, de 15 de octubre de 2018, en sus artículos 37 a 40, realiza actualizaciones a la normativa de protección de datos personales e incorpora nuevas tendencias internacionales en la materia. Su finalidad fue contemplar el avance de la tecnología y el nuevo contexto que esto apareja, y adoptar las mejores soluciones internacionales para dar respuesta adecuada a los titulares de los datos personales.

Es así entonces que se incorporan como elementos nuevos el concepto de extraterritorialidad, el de vulneraciones de seguridad, el de responsabilidad proactiva (que incluye la realización de evaluaciones de impacto, adopción de medidas de privacidad por diseño y por defecto), así como la creación de la figura del delegado de protección de datos para determinadas situaciones.

A dichos efectos, y para poder ampliar los conceptos que se incorporaron a la normativa de protección de datos, se reglamentaron los artículos indicados por Decreto Nº 64/020, de 17 de febrero de 2020.

Una relación del contenido del decreto, y su texto pueden encontrarse en la 5ª. Edición de la Revista de Protección de Datos Personales, disponible en la página web de la Unidad.

Datos biométricos

Los artículos 86 y 87 de la Ley N° 19.924, de 18 de diciembre de 2020, introducen en la legislación nacional el concepto de "datos biométricos", incorporando un literal Ñ al artículo 4° de la Ley N° 18.331, de 11 de agosto de 2008, y estableciendo que previo a toda operación de tratamiento de estos datos deberá realizarse una evaluación de impacto en la protección de datos personales (para lo que se incorporó a la ley citada el artículo 18 bis).

Con respecto a estas modificaciones, se está elevando a rango legal una obligación que ya había sido impuesta por la Unidad por Resolución N° 30/020, de 12 de mayo de 2020, en ejercicio de las competencias que se le otorgaron por el artículo 6° literal g del decreto N° 64/020.

En cuanto al concepto de datos biométricos, la legislación uruguaya ahora lo reconoce como: "*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona tales como datos dactiloscópicos, reconocimiento de imagen o voz*".

JURISPRUDENCIA INTERNACIONAL

El Tribunal de justicia de la Unión Europea declara inválida la decisión que permitía a las transferencias en base al escudo de privacidad

En una decisión con efectos internacionales, el Tribunal de Justicia de la Unión Europea, mediante la sentencia de 16 de julio de 2020 (asunto C-311/18), invalida la Decisión 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU mientras que declara que la Decisión 2010/87 de la Comisión,

relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, es válida.

El Tribunal indica que si el Pr Privacy Shield no confiere a los interesados derechos exigibles a las autoridades estadounidenses ante los tribunales. Por tanto**,** no proporciona a las personas ninguna vía de recurso ante un órgano que ofrezca garantías sustancialmente equivalentes a las exigidas en el Derecho de la Unión**,** que puedan asegurar tanto la independencia del Defensor del Pueblo previsto en el antedicho mecanismo como la existencia de normas que faculten al referido Defensor del Pueblo para adoptar decisiones vinculantes con respecto a los servicios de inteligencia estadounidenses.

Acceder a la sentencia

El Tribunal de justicia de la Unión Europea de expide respecto al consentimiento otorgado en casillas marcadas antes a la firma del contrato

En su sentencia de fecha 11 de noviembre, en el asunto C-61/19, el Tribunal de Justicia de la Unión Europea establece que no es válido el consentimiento otorgado por un cliente para la obtención y la conservación de sus datos personales cuando la casilla había sido marcada antes de la firma del contrato por el responsable del tratamiento de la compañía demandada.

En el caso, una compañía que presta servicios de telecomunicaciones en el mercado de móviles rumano obtuvo y conservó copias de los documentos de identidad de sus clientes sin el consentimiento expreso de éstos. Según las verificaciones efectuadas por el órgano jurisdiccional remitente, existen, por un lado, contratos en los que se ha insertado una cruz en la casilla correspondiente a la cláusula relativa a la conservación de copias de documentos que contienen datos personales con fines de identificación y, por otro, contratos en los no figura esa cruz. Ante ello, el Tribunal de Distrito de Bucarest solicitó al Tribunal de Justicia que precisara las condiciones en las que puede considerarse válido el consentimiento de los clientes para el tratamiento de datos personales.

En primer lugar, la justicia europea recuerda que el Derecho de la Unión no admite como válido el consentimiento de tratamiento de datos personales en caso de silencio**,** de casillas ya marcadas o de inacción del interesado, sino que dicho consentimiento debe ser libre, específico, informado e inequívoco.

Acceder a la sentencia

DIFUSIÓN Y CAPACITACIÓN DE LA UNIDAD

Sitio web

En el año 2020, en virtud de la emergencia sanitaria declarada, 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 2020 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.

Charlas de café

Nuevas obligaciones en materia de protección de datos

La primera Charla de Café se realizó el 24 de junio. Dicha instancia contó con la participación de 134 personas y estuvo a cargo del Dr. Felipe Rotondo, presidente del Consejo Ejecutivo de URCDP; los integrantes de la unidad Dres. Gonzalo Sosa, Beatriz Rodríguez, Flavia Baladán y Lylian Massarino; y la Ing. Virginia Pardo.

Uno de los temas abordados fue la ampliación del ámbito territorial de la ley uruguaya, que ahora también alcanza a quienes desde el exterior ofrecen productos o servicios a habitantes del país o realizan el análisis de su comportamiento, entre otros, según lo especificado en el Decreto N° 64/020.

También se trató el régimen de comunicación de vulneraciones de seguridad y se detallaron las medidas preventivas, los plazos y el trabajo conjunto entre la unidad y el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (Cert Uy).

Asimismo, fueron analizadas las medidas de responsabilidad proactiva, en especial, las evaluaciones de impacto. En este sentido, se comentó la regulación del Decreto N° 64/020, la Resolución N° 30/020 sobre datos biométricos y la Guía de evaluaciones de impacto publicada por la unidad y la Agencia de Acceso a la Información Pública de Argentina.

Por último, se analizó la figura del delegado de Protección de Datos, los requisitos de la reglamentación (incluyendo los casos de delegados personas jurídicas y de equipos multidisciplinarios) y la Resolución N° 32/020, que especifica las condiciones para ser delegado y la forma de comunicar su designación.

Datos personales más allá del principio de finalidad

La segunda Charla de Café se realizó el 12 de agosto. Dicha actividad contó con la participación de más de 90 personas y estuvo a cargo del equipo jurídico de la Unidad de Protección de Datos Personales. Se contó con la presencia de Hebert Paguas, director ejecutivo de Agesic, el Dr. Felipe Rotondo, presidente del Consejo Ejecutivo y la Ing, Virginia Pardo, directora del área de Sociedad de la Información de Agesic.

Durante la jornada se expuso sobre distintas problemáticas relacionadas con el uso de información personal, con fines distintos a los que motivaron su recolección original. Se hizo especial referencia al uso de la información con fines científicos y estadísticos y los mecanismos asociados a la ciencia de datos.

También se trató la vinculación entre los derechos de protección de datos, la propiedad intelectual y la necesidad de buscar los medios para contemplarlos.

Para trabajar las diferentes temáticas, se consideró el marco de dictámenes y resoluciones del Consejo Ejecutivo de la URCDP, que fueron expuestos en la charla.

Datos Biométricos

El 17 de diciembre se realizó la última charla de café del 2020, a cargo del equipo jurídico de la Unidad. Durante la actividad se manejaron los distintos conceptos de "dato biométrico" y la postura del Consejo Ejecutivo, reflejado en la última resolución al respecto, además de la propuesta incluida en el proyecto de ley de presupuesto, que establece dentro de la Ley N° 18.331, de 11 de agosto de 2008 una nueva definición y una regulación particular.

Por otra parte, se relevaron las distintas regulaciones a nivel internacional y la forma de encarar el tratamiento de estos datos (con particular referencia al Reglamento General Europeo de Protección de Datos).

Finalmente, se analizó la obligación de realizar una evaluación de impacto en la protección de datos personales además de otras medidas de responsabilidad proactiva, y en particular se indicó que existe disponible una guía para evaluaciones de impacto en la página web de la Unidad.

Curso de Protección de Datos Personales para funcionarios

La URCDP continuó con el dictado de una serie de ediciones del curso de Protección Datos Personales dirigido a funcionarios públicos de diversas entidades del Estado.

En el curso los temas abordados incluyeron una aproximación a la situación de la protección de datos a nivel nacional e internacional, el análisis de las normas que regulan la materia en nuestro país y el estudio de casos prácticos de relevancia en base a expedientes llevados adelante por la Unidad, entre otros.

El curso se dividió en cinco instancias de dos horas de duración cada una, y fue dictado por asesores de la Unidad a través de presentaciones e intercambio con los participantes.

Curso de delegados

Se desarrolló la primera edición del Curso para Delegados de Protección de Datos, el cual se desarrolló entre los meses de abril y de mayo y contó con una importante presencia de delegados del ámbito privado.

En el curso se brindaron herramientas para el desarrollo de la tarea, se explicaron los temas más complejos en la materia y se profundizó en cuestiones interés para la protección de datos.

RELACIONAMIENTO INTERNACIONAL

Participación en grupos de la Asamblea Global de Privacidad

La Asamblea Global de Privacidad 2020, prevista para el mes de octubre en México, debió ser cancelada a causa de la pandemia. No obstante, se mantuvo el trabajo de las autoridades participantes en los distintos Grupos de Trabajo en temáticas asociadas a la protección de datos personales.

En el correr del año 2020 la Unidad participó activamente en el Grupo de Trabajo en Estándares Internacionales, liderado por la autoridad de protección de datos de Reino Unido, que realizó reuniones periódicas en el correr del año 2020, para culminar con un documento en el que se realiza una comparación de los distintos esquemas de protección de datos disponibles.

Además, participó especialmente en el Grupo de Trabajo sobre COVID 19 liderado por la autoridad de Filipinas, en el que se trataron distintos aspectos de la gestión de la pandemia, y se realizaron varios talleres virtuales en la materia junto con otras autoridades miembros de la GPA y expertos internacionales.

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

Debido a la pandemia, las reuniones plenarias y del Bureau del Consejo Consultivo del Convenio 108 se realizaron de forma virtual en el correr del año 2020. La reunión plenaria del mes de julio debió cancelarse a causa de la pandemia, en tanto la prevista para el 18 a 20 de noviembre se realizó de forma remota.

En la citada reunión de noviembre de trataron diversos temas, entre los que se encontró la elección de los miembros del Bureau, por el plazo de 2 años. El coordinador de la Unidad, Gonzalo Sosa Barreto, fue electo como uno de los miembros, junto a representantes de Italia, Georgia, Senegal, Alemania, Federación Rusa y Suiza.

El Bureau del Convenio tiene a su cargo la revisión de la documentación preparada por la Secretaría en forma previa a su presentación en el plenario de la conferencia, validar las decisiones en materia de formalización de los distintos procesos de aprobación de la documentación, entre otros.

Participación en la Red Iberoamericana de Protección de Datos Personales

En el año 2020 Uruguay culminó su participación con Presidente de la Red Iberoamericana de Protección de Datos, luego de su elección en el año 2016 y

reelección en el año 2018, manteniéndose como miembro del Comité Ejecutivo de la Red.

La elección de la nueva Presidencia de la Red Iberoamericana, que recayó en la Secretaría de Industria y Comercio de Colombia, y de los restantes miembros del Comité Ejecutivo (autoridades de Argentina, México y Uruguay) se efectuó en ocasión del XVIII Encuentro Iberoamericano de Protección de Datos el día viernes 4 de diciembre de 2020 desde Montevideo.

En dicho Encuentro, Uruguay realizó el informe anual de la Presidencia; se destacó especialmente el cumplimiento de los objetivos previstos en el documento estratégico RIPD 2020, y se presentó y aprobó el nuevo plan estratégico hasta el año 2025.

La designación del nuevo Comité Ejecutivo se realizó en la sesión cerrada del Encuentro, donde se aprobó además la declaración final.

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

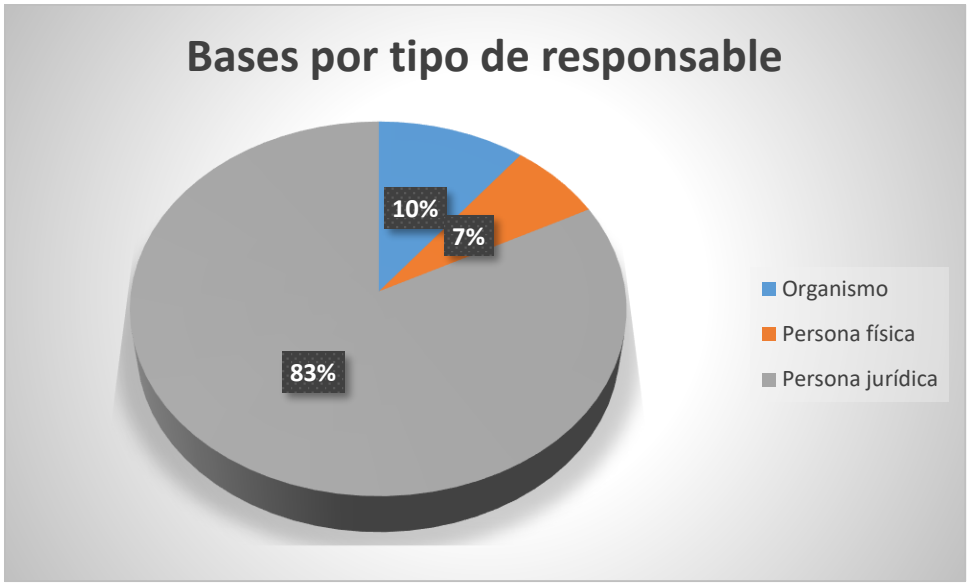
En abril de 2016 se puso a disposición de los responsables de bases de datos un sistema totalmente informatizado que permite el envío y formalización de todos los procedimientos necesarios para la inscripción definitiva de las bases en el registro que lleva adelante la unidad. En el año 2018 se procedió a la migración de todos los procesos de inscripción de bases de datos, que son analizadas y expedidas íntegramente por el citado sistema.

En las tablas y gráficos siguientes se presentan los resultados del registro online de los formularios ingresados y los aprobados durante el año 2020.

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 2020, discriminadas por tipo de responsables.

Cantidad de bases inscriptas por responsable – Año 2020



Debe tenerse presente que, a partir de la implementación del nuevo sistema, las resoluciones de inscripción de bases de datos 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-videovigilancia

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.

Porcentaje en cantidad de bases de videovigilancia inscriptas por nuevo Sistema – Año 2020

Transferencias internacionales

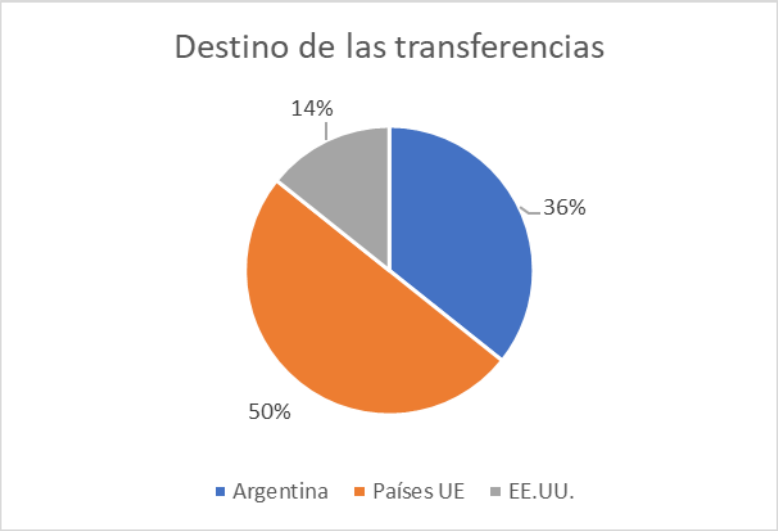
Las transferencias internacionales de datos se encuentran habilitadas por las normas en materia de Protección de Datos, siempre bajo el cumplimiento de determinados requisitos y la autorización previa de la unidad, salvo contadas excepciones. Durante 2018 se declararon transferencias internacionales en un 12% de las bases de datos.

Uruguay y Argentina son los únicos países latinoamericanos declarados adecuados por decisión del Parlamento y la Comisión Europea, lo que permite la transferencia libre de datos entre la Unión Europea y nuestro país. Ello no se ve modificado por la entrada en vigencia del nuevo Reglamento General de Protección de Datos. Con respecto a las transferencias con los Estados Unidos de América, la Comisión Europea adoptó en julio de 2016 la decisión referente a la instauración de un Privacy Shield (o “Escudo de Privacidad”) a efectos de proteger los datos personales de las personas que se encuentran en la Unión Europea. Dicha decisión fue dejada sin efecto por sentencia del Tribunal de Justicia de la Unión Europea el 16 de julio de 2020, encontrándose actualmente en proceso de revisión el mecanismo de habilitación de transferencias al citado país.

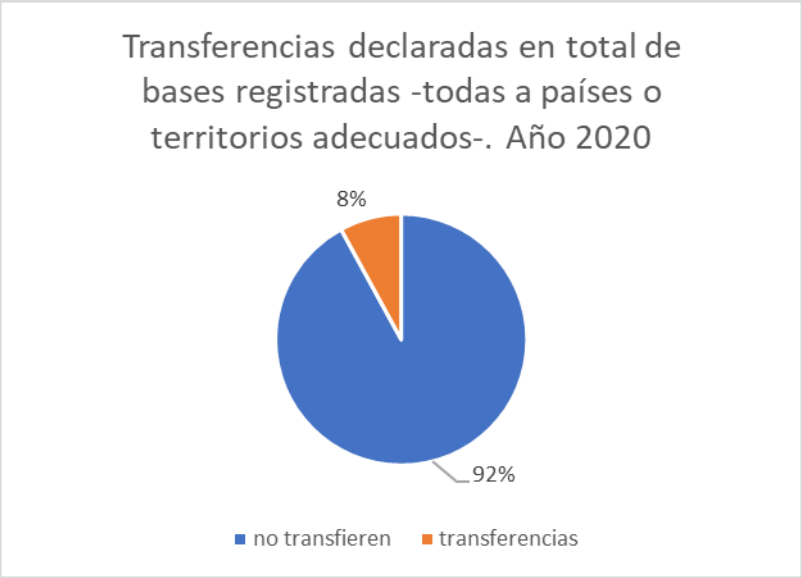
Por Resolución del Consejo Ejecutivo N° 4/019, de 12 de marzo de 2019, nuestro país ha determinado los países que se consideran adecuados a los efectos de habilitar transferencias internacionales, en concreto, los miembros de la Unión Europea y el Espacio Económico Europeo, Principado de Andorra, República Argentina, el sector privado de Canadá, 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.. La resolución se encuentra disponible en el sitio web de la Unidad.

Las transferencias a países no adecuados requieren del cumplimiento de las exigencias legalmente definidas en el artículo 23 de la Ley N° 18.331, de 11 de agosto de 2008, y en su caso, la solicitud de una autorización expresa de la unidad, ya sea para una transferencia en particular o un conjunto de transferencias. A este respecto, en el año 2020 no se solicitaron autorizaciones especiales para la realización de transferencias a países no adecuados. Se destaca la realización de transferencias a Argentina, Países de la Unión Europea y Estados Unidos.

Transferencias internacionales por destino



Transferencias internacionales sobre bases registradas – Año 2020



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.

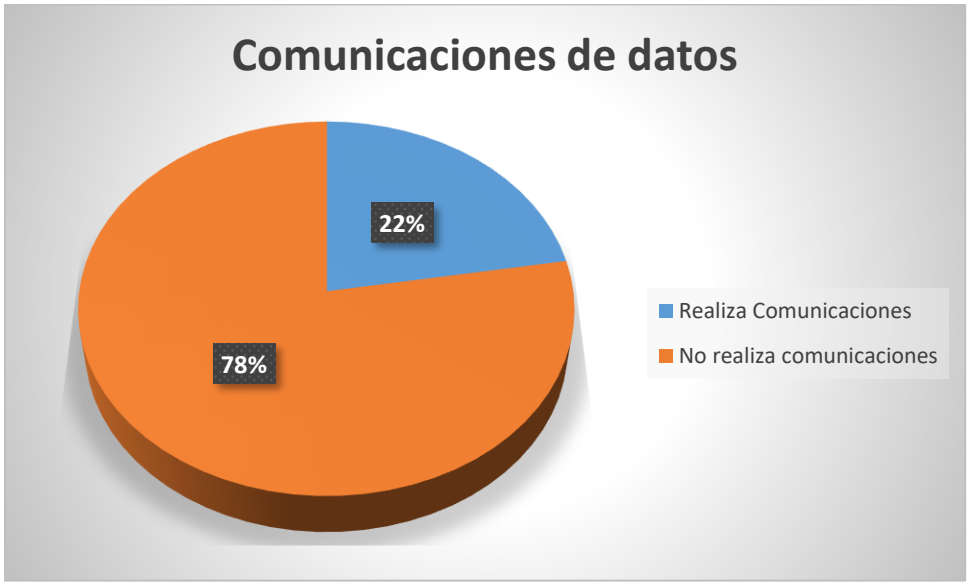
· Datos de bases de datos con fines de publicidad.

· 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 2020 asciende a un 22%, 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 2020



Tipo de soporte de registro de base de datos

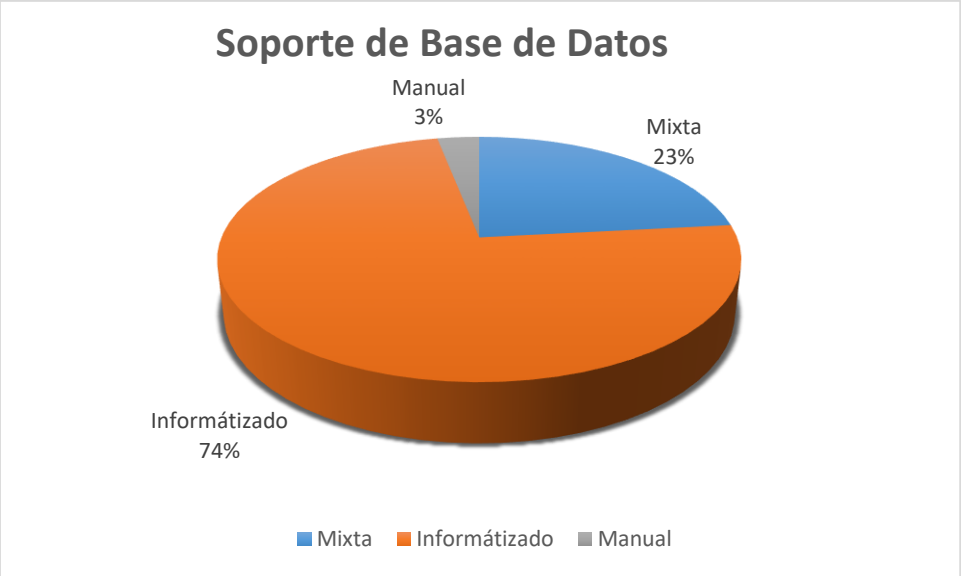
Los soportes utilizados para las bases de datos registradas son:

· Manual.

· Informatizado.

· Manual e informatizado (mixta).

· Otros.



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 2020 se aprobaron tres 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 2020 se recibieron a través del sistema puesto a disposición por la Unidad para tal fin, un total de 66 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.

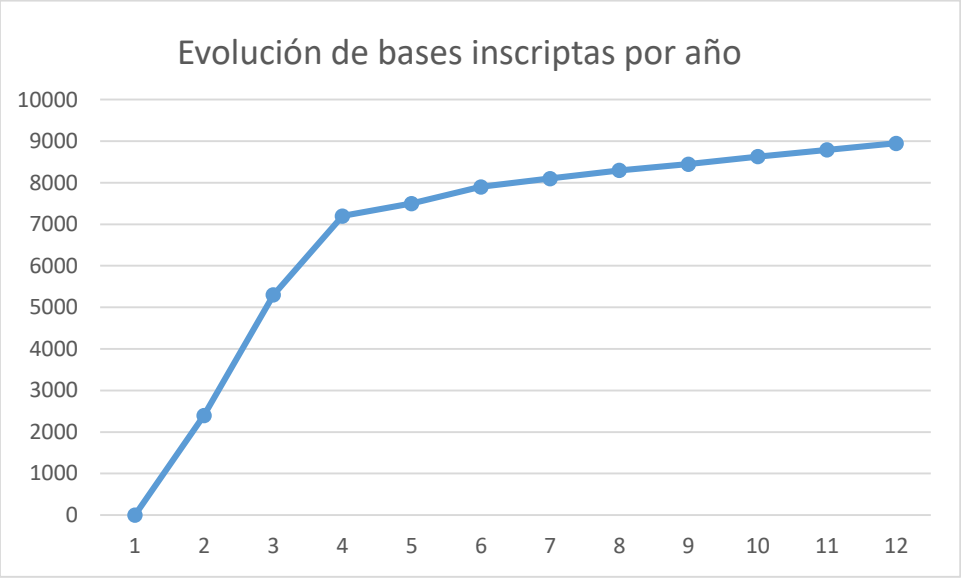
Valoración jurídica: Un abogado evalúa el cumplimiento de los requerimientos sustanciales previstos por la normativa nacional vigente, solicitando, en caso de eventuales inconsistencias, las aclaraciones que se estimen pertinentes. Este proceso se ha simplificado gracias a la asistencia del sistema informático, 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.

El siguiente gráfico muestra la evolución anual de bases de datos inscriptas.

Evolución de bases de datos inscriptas desde 2009 a 2020



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. Durante el año 2020 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 2020, la URCDP recibió 32 consultas, 101 denuncias y 8 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 2020 se aplicaron 14 observaciones, 24 apercibimientos y 8 multas y se realizaron intimaciones y exhortaciones a 20 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 2020 se analizaron los expedientes presentados ante la URCDP, además de otros aspectos derivados de la pandemia, y se constató la expedición de 62 resoluciones y 18 dictámenes.

Las personas pueden tener acceso a toda la información a través del sitio web de la URCDP.

Cantidad de informes realizados

En función de los requerimientos que ha recibido la URCDP, se han elaborado 815 informes (328 notariales y 487 sobre denuncias, consultas y registro de base de datos), que incluyen los puntos de vista jurídico, notarial y técnico referidos anteriormente.