UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

MEMORIA ANUAL
2016

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

MEMORIA ANUAL
2016

ÍNDICE

PRÓLOGO 5

01. PRIMERA SEMANA NACIONAL DE PROTECCIÓN DE DATOS PERSONALES 7

CAMPAÑA NACIONAL DE PROTECCIÓN DE DATOS PERSONALES "TUS DATOS VALEN. CUIDALOS" 8

ACTIVIDADES ACADÉMICAS 11

MONTEVIDEO 11

MALDONADO 11

REVISTA DE PDP 12

PRESENTACIÓN DE LA MEMORIA 2015 13

CRITERIOS ADMINISTRATIVOS 2009-2015 14

02. PRINCIPALES TEMAS ANALIZADOS EN EL AÑO 15

EJERCICIO DE LOS DERECHOS CONSAGRADOS EN LA LEY N° 18.331 16

COMUNICACIÓN DE DATOS – PRUEBA EN PROCESO JUDICIAL 16

COMUNICACIÓN DE DATOS – INTERCAMBIO DE INFORMACIÓN 16

PUBLICACIONES EN INTERNET 17

PUBLICACIÓN EN INTERNET DE INFORMACIÓN PERSONAL EN GENERAL 17

PUBLICACIÓN EN INTERNET POR PARTE DE ORGANISMOS PÚBLICOS 17

PUBLICACIÓN EN INTERNET DE INFORMACIÓN A TRAVÉS DE ORGANISMOS ENCARGADOS DE PUBLICACIONES OFICIALES 18

03. AVANCES NORMATIVOS 19

3.1 NORMATIVA INTERNACIONAL 20

3.2 INFORME SOBRE AVANCES NORMATIVOS 20

04. INFORMES DE INTERÉS 27

INFORME VINCULADO CON LA IMPLEMENTACIÓN DE UN SOFTWARE DE REGISTRO ÚNICO DE USUARIOS CON VIH 28

05. SENTENCIAS INTERNACIONALES DE INTERÉS 45

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA 46

06. DIFUSIÓN Y CAPACITACIÓN DE LA URCDP 47

SITIO WEB 48

ATENCIÓN DE CONSULTAS PERSONALIZADAS 48

CURSO DE PROTECCIÓN DE DATOS EN LÍNEA 48

CHARLAS DE CAFÉ 49

"EDUCACIÓN Y PROTECCIÓN DE DATOS" 50

"IDENTIDAD DIGITAL Y PROTECCIÓN DE DATOS" 51

"INNOVACIONES TECNOLÓGICAS Y PROTECCIÓN DE DATOS PERSONALES: CIUDADES INTELIGENTES E INTERNET DE LAS COSAS" 52

FILM *DEMOCRACY* Y EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS PERSONALES 53

CHARLAS IMPARTIDAS EN 2016 A DIFERENTES ENTIDADES 54
REDES DE REPLICACIÓN 54

07. RELACIONAMIENTO INTERNACIONAL 55

PRESIDENCIA DE LA RIPD 56
SIMPOSIO SOBRE CIBERSEGURIDAD Y PRIVACIDAD EN LATINOAMÉRICA Y GLOBAL PRIVACY SUMMIT 2016 56
XIV ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS Y EL IV CONGRESO INTERNACIONAL DE PROTECCIÓN DE DATOS 57
IV REUNIÓN DEL COMITÉ AD HOC DE PROTECCIÓN DE DATOS (CAHDATA) 57
33ª REUNIÓN PLENARIA DEL COMITÉ CONSULTIVO DEL CONVENIO Nº 108 DEL CONSEJO DE EUROPA. 58
38ª CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD 59
SEMINARIO "DERECHO AL OLVIDO, TUTELA INTEGRAL DE LA PRIVACIDAD. VISIÓN IBEROAMERICANA" 60
FORO DE AUTORIDADES DE PRIVACIDAD DE ASIA PACÍFICO (APPA) 60
ENCUENTRO CON REFERENTES ACADÉMICOS Y AUTORIDADES DE PROTECCIÓN DE DATOS 61

08. LA URCDP EN CIFRAS 65

REGISTRO DE DATOS PERSONALES DE ACUERDO CON EL TIPO DE RESPONSABLE 66
DATOS ESPECIALMENTE PROTEGIDOS 68
TRANSFERENCIAS INTERNACIONALES 69
TIPO DE INFORMACIÓN SEGÚN SU FINALIDAD 70
CESIONES O COMUNICACIONES DE DATOS 72
TIPO DE SOPORTE DE REGISTRO DE BASE DE DATOS 72
CÓDIGOS DE CONDUCTA 72
BASES DE DATOS INSCRIPTAS ANTE LA URCDP 73
CONSULTAS A LA MESA DE AYUDA DE LA URCDP 74
EXPEDIENTES PRESENTADOS POR CONSULTAS Y DENUNCIAS 75
RESOLUCIONES QUE IMPONEN SANCIONES 75
RESOLUCIONES Y DICTÁMENES REALIZADOS EN 2016 76
CANTIDAD DE INFORMES REALIZADOS 76
09 77

09. LA URCDP ANTE LOS NUEVOS RETOS EN MATERIA DE PROTECCIÓN DE DATOS 77

PROMOCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS 78
GOBERNANZA Y FORTALECIMIENTO DE CAPACIDADES 78
FORTALECIMIENTO Y POSICIONAMIENTO DE LA UNIDAD 79
RELACIONAMIENTO INTERNACIONAL 80

PRÓLOGO

La Unidad Reguladora y de Control de Datos Personales presenta su *Memoria* correspondiente al año 2016 con la finalidad de informar sobre las actividades desarrolladas en el período, en ejecución de los cometidos que le asigna la Ley Nº 18.331 de 11 de agosto de 2008.

Se incluye, entonces, una recopilación de esas actividades, las cuales mantienen los lineamientos de años anteriores, si bien debe precisarse que, en virtud de los asuntos tratados y la incidencia que en ellos tienen las nuevas tecnologías, presencia de innovación en permanente sucesión, ya se ha encarado la materia de protección de datos personales en una visión de futuro, tal como lo ha sido en el ámbito de la Unión Europea a través del Reglamento General aprobado el 27 de abril de 2016. Esta cuestión se proyectará en acciones que van más allá de esta *Memoria*.

Una vez más se subraya que siempre se ha tenido presente el valor esencial del derecho fundamental, inherente a la personalidad humana, que constituye el debido tratamiento de los datos personales.

Con ese fundamento, se siguió con las actividades de acercamiento a los menores de edad a través del concurso para niños y niñas de 5º y 6º año de escuelas públicas y privadas denominado "Tus datos, tu decisión", en esta ocasión basado en cuentos cortos. Tal como en concursos de años anteriores, se tuvo el apoyo de Anep-Consejo de Educación Inicial y Primaria, IMPO y Plan Ceibal.

De la misma manera, se continuó con la capacitación de funcionarios de distintas instituciones y en diversas áreas del país, así como con la evacuación de consultas y expedición de un importante número de dictámenes y resoluciones sobre temas en materia de protección de datos personales.

Se inició la realización de encuentros con convocatoria abierta y un encare "descontracturado" a los que se denominó "Charlas de Café"; en ellos, se trataron en 2016 cuestiones de interés, específicamente, las relativas a la relación de la protección de Datos Personales con la educación, la identidad digital y las innovaciones tecnológicas (ciudades inteligentes e internet de las cosas).

Asimismo, en oportunidad de conmemorarse la fecha de promulgación de la Ley Nº 18.331, se efectuó la "Primera Semana Nacional de Protección de Datos Personales", actividad académica en la que intervinieron expertos nacionales y extranjeros y que se extendió al departamento de Maldonado.

Esa semana fue marco para la presentación de la Revista de Protección de Datos Personales de la URCDP a través de su primer número, el cual incluyó ponencias de expertos de diversos países y documentación de fuente jurisprudencial y administrativa.
A nivel internacional, se continuó con la participación en la actualización del Convenio Nº 108 del Consejo de Europa "para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", del cual el Uruguay forma parte.

En el ámbito iberoamericano, por decisión adoptada en noviembre 2016, nuestro país, a través de la Unidad, preside la Red Iberoamericana de Protección de Datos Personales, "foro permanente de intercambio de información abierto a todos los países miembros de la comunidad iberoamericana" que se creara en el Encuentro Iberoamericano celebrado en La Antigua, Guatemala, en junio de 2003.

La presente *Memoria* está, pues, dirigida a permitir apreciar la labor realizada en el período en una materia de interés general, el cual comprende, por esencia, el respeto de los derechos de las personas, entre ellos, a la protección de datos personales.

Dr. Felipe Rotondo

01

PRIMERA SEMANA NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

En el marco del impulso a la difusión del derecho a la protección de datos que ha caracterizado a la URCDP y con el objetivo de celebrar los ocho años desde la promulgación de la Ley Nº 18.331, de 11 de agosto de 2008, se organizó en la semana comprendida entre el 8 y el 12 de agosto la "Primera Semana Nacional de la Protección de Datos Personales", que contó con varias actividades y la participación de múltiples actores sociales.

CAMPAÑA NACIONAL DE PROTECCIÓN DE DATOS PERSONALES "TUS DATOS VALEN. CUIDALOS"

Continuando con la tradicional campaña nacional de protección de datos "Tus Datos Valen", se desarrolló la cuarta edición del concurso escolar denominado "Tus datos cuentan". Este año, la consigna propuso que alumnos de 5º y 6º años de escuelas públicas y privadas de todo el país identificaran y resolvieran, a través de la redacción de un cuento corto, situaciones en las cuales el uso de los datos personales, ya sean propios o de terceros, estuviera en juego.

Nuevamente, se contó con el apoyo de la Administración Nacional de Educación Pública (Anep), la Dirección Nacional de Impresiones y Publicaciones Oficiales (Impo), el Consejo de Educación Inicial y Primaria (Ceip-Anep), Plan Ceibal, la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic) y Presidencia de la República.

En el concurso participaron representantes de quince departamentos del país, quienes hicieron llegar un total de sesenta y dos cuentos. Una clase de la Escuela N°17 de Vergara, Treinta y Tres, fue la ganadora del primer premio.

Los cuentos ganadores se encuentran disponibles en la página web de la URCDP.

Ganadores

- 1er premio: “Como pompas de jabón”. Escuela N° 17, Vergara, Treinta y Tres.
- 2do premio: “Alicia en el país de la tecnología”. Escuela N° 2, Paysandú.
- 3er premio: “Las vacaciones inolvidables”. Escuela N° 60, La Mina, Cerro Largo.

Asimismo, se entregaron algunas menciones especiales:

Mención especial por originalidad y creatividad

- “Una Cenicienta moderna”. Escuela N° 18, Trinidad, Flores.
- “La caída de un genio”. Escuela N° 78, Queguayar, Paysandú.
- “Datos espaciales”. Escuela N° 3, Trinidad, Flores.

Como pompas de jabón...
Primer premio

Alicia en el país de la tecnología
Segundo premio

Las vacaciones inolvidables
Tercer premio

ACTIVIDADES ACADÉMICAS

Las actividades académicas realizadas en el marco de la Primera Semana Nacional de Protección de Datos Personales, bajo la consigna: "Retos de la privacidad en la sociedad de la información", se realizaron en Montevideo y Maldonado con el objetivo de reflexionar en torno a los nuevos desafíos del derecho a la protección de datos personales en el contexto de las nuevas realidades operativas y normativas del mundo de las TIC.

MONTEVIDEO

Además de la entrega de los premios del concurso "Tus Datos Valen", se realizó una Conferencia Internacional en Montevideo los días 9 y 10 de agosto.

En el evento se trataron temas vinculados con la protección de datos en Iberoamérica, como el derecho al olvido, realizándose consideraciones asociadas con la sentencia europea relacionada con dicho derecho y su aplicación a la realidad latinoamericana; las nuevas disposiciones normativas internacionales, destacándose la aprobación del nuevo Reglamento General de Protección de Datos europeo y la modernización del Convenio 108 del Consejo de Europa; la ponderación de derechos fundamentales, analizándose desde una perspectiva global la pertinencia de aplicar el derecho a la protección de datos y su vínculo con otros derechos fundamentales; la elaboración de perfiles desde las perspectivas comercial, estatal, social y económica, considerándose además el tratamiento masivo de información; las perspectivas sobre el tratamiento de información personal desde el punto de vista de la educación, la salud y la actividad comercial; y los desafíos de la protección de datos según las Autoridades de Control.

En el cierre de las jornadas realizadas en Montevideo, el presidente del Consejo Ejecutivo destacó el involucramiento de integrantes de otros organismos, la academia y la sociedad civil, subrayando la importancia de la educación y la difusión del derecho.

Se contó con la participación de profesionales, autoridades y académicos de distintos países de América Latina, destacándose la presencia del Dr. Eduardo Bertoni, director de la Dirección de Protección de Datos de la República Argentina, el Mag. Gustavo Parra Noriega, coordinador de Protección de Datos del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos de los Estados Unidos Mexicanos, el Dr. Danilo Doneda, académico de la Universidad de Río de Janeiro, República Federativa del Brasil, y el Dr. Pablo Palazzi, académico de la Universidad San Andrés, de la República Argentina.

MALDONADO

El 11 de agosto, en el Campus de Maldonado, concluyó la 1ª Semana Nacional de Protección de Datos Personales con la participación del Consejo Ejecutivo de la URCDP y la Intendencia de Maldonado.

Durante la jornada se desarrollaron mesas y paneles acerca de temas tales como "Derechos fundamentales en la Sociedad de la Información", "Redes sociales y protección de datos" e "Impacto de la protección de datos en la actividad estatal".

En el primero de los paneles se analizaron cuestiones vinculadas con la ponderación de los derechos fundamentales a la protección de los datos personales y el acceso a la información pública, para lo cual se contó con la participación de representantes de la

academia y de las Unidades de Protección de Datos Personales y Acceso a la Información Pública.

El segundo panel permitió analizar los desafíos para la protección de datos ante el avance de las redes sociales en la vida cotidiana de las personas, en especial, entre los menores de edad.

Finalmente, en el tercer panel se discutió el impacto de la protección de datos en cuestiones tales como el intercambio de información, el consentimiento informado y las políticas de privacidad.

REVISTA DE PDP

En el "Prólogo" del número inicial de la *Revista Uruguaya de Protección de Datos Personales* se expresa que la publicación constituye una "iniciativa de la Unidad Reguladora y de Control de Datos Personales de encarar una nueva vía de difundir los derechos que garantiza el régimen de la Ley Nº 18.331, de 11 de agosto de 2008, e incentivar su conocimiento y debida aplicación".

Se recogen en la revista trabajos doctrinarios de importantes autores nacionales y extranjeros, complementados con jurisprudencia, dictámenes de la URCDP, notas de interés y entrevistas.

En la sección "Doctrina" se contó con los aportes de Chantal Bernier, ex comisionada de Privacidad Interina y comisionada adjunta de la Oficina del Comisionado de Privacidad de Canadá; Giovanni Buttarelli, supervisor europeo de Protección de Datos; Carlos Delpiazzo, exdecano de la Facultad de Derecho de la Universidad Católica del Uruguay; Mar España Martí, directora de la Agencia Española de Protección de Datos; Pablo Palazzi, profesor de Derecho de la Universidad de San Andrés; Ximena Puente de la Mora, expresidente del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos de México; y Ahti Saarenpaa, profesor emérito de Derecho Privado en la Universidad de Laponia. Asimismo, se realizó una entrevista a Jacob Kohnstamm, ex presidente de la Autoridad Holandesa de Protección de Datos; y hubo también una nota de interés realizada por María Verónica Pérez Asinari, jefa de la Unidad de Supervisión y Aplicación de la ley de la Oficina del Supervisor Europeo de Protección de Datos.

PRESENTACIÓN DE LA MEMORIA 2015

En el marco de las actividades reseñadas, se realizó la presentación de la Memoria Anual 2015 de la URCDP.

Se destacan en esta edición las múltiples actividades de capacitación realizadas, los concursos para escolares y los dictámenes y resoluciones adoptados por la unidad a partir de las consultas y denuncias realizadas.

El presidente del Consejo de la URCDP señaló la importancia de elaborar una memoria anual no como un medio para destacar logros, sino como el reflejo de un ejercicio republicano de transparencia y rendición de cuentas acerca de lo actuado en el año.

CRITERIOS ADMINISTRATIVOS 2009-2015

Por primera vez en la historia de la unidad se publicó una recopilación de los principales criterios definidos por el Consejo Ejecutivo a través de las resoluciones y dictámenes emitidos desde su creación.

El objetivo de la publicación es realizar un aporte para el conocimiento y protección del derecho, en el marco de las actividades de promoción que ha venido llevando adelante la URCDP.

Se recopilan así criterios asociados a transferencias internacionales, comunicación de datos a terceros, tratamiento de datos para publicidad y marketing, tratamiento de datos por entidades públicas, datos personales y fuentes públicas, registro de bases de datos, ejercicio de derechos, tratamiento de datos sensibles, videovigilancia, tratamiento de datos en la nube y sistema de sanciones.

02

PRINCIPALES TEMAS ANALIZADOS EN EL AÑO

EJERCICIO DE LOS DERECHOS CONSAGRADOS EN LA LEY Nº 18.331

Por Resolución Nº 1/016, de 17 de febrero, se sancionó a la denunciada con apercibimiento por no haber dado cumplimiento a las previsiones de la ley en materia de actualización de información de una deuda del denunciante. En el caso concreto, la denunciada demoró más de ocho meses en actualizar la información cuando la ley prevé un plazo de cinco días hábiles. Similares situaciones fueron consideradas por el Consejo Ejecutivo en las Resoluciones Nos. 84/016, de 23 de noviembre, y 91/016, de 22 de diciembre, que resultaron en sanciones para las denunciadas.

Asimismo, y por Resolución Nº 32/016, de 8 de junio, se procedió a sancionar con apercibimiento a un denunciado por no haber permitido el ejercicio del derecho de supresión al denunciante, conforme lo dispuesto por el artículo 15 de la ley, aún cuando este último lo solicitó expresamente y obtuvo una respuesta favorable del primero.

COMUNICACIÓN DE DATOS – PRUEBA EN PROCESO JUDICIAL

Por Resolución Nº 21/016, de 27 de abril, se apercibió a una profesional abogada y a su cliente por comunicación de datos relativos a la actividad comercial y crediticia de una tercera persona, cónyuge del cliente, sin su consentimiento. El Consejo consideró que los datos relativos a la actividad comercial o crediticia de las personas son información personal especialmente protegida y para su obtención y comunicación se requiere del previo consentimiento informado del titular, salvo excepciones. Se evaluó, además, que el acceso a la información por personas distintas al titular del dato obedece a la existencia de un contrato con la empresa que lo provee y su utilización debe restringirse a la finalidad contractual, requiriéndose para cualquier uso distinto por parte del destinatario el previo consentimiento informado del titular, incumpliéndose en el caso los artículos 9º, 17 y 22 de la Ley Nº 18.331.

COMUNICACIÓN DE DATOS – INTERCAMBIO DE INFORMACIÓN

Por Dictamen Nº 15/016, de 8 de setiembre, se consideró como ajustada a la Ley Nº 18.331 la comunicación de información a una facultad por parte de un organismo encargado de proveer ayuda económica a estudiantes, a efectos de realizar un seguimiento personalizado de los estudiantes becados. A tales efectos, se evaluaron las disposiciones legales aplicables a la materia y a las instituciones involucradas en el intercambio de información.

Por Dictamen Nº 20/016, de 23 de noviembre, el Consejo Ejecutivo entendió que en la comunicación de datos sensibles, como el diagnóstico de una enfermedad, corresponde la aplicación del artículo 18 de la ley, no existiendo en la situación planteada un mandato legal o interés general que justifique dicha comunicación.

PUBLICACIONES EN INTERNET

El Consejo Ejecutivo de la URCDP se ha pronunciado en múltiples oportunidades en el curso del año 2016 respecto a la publicación en internet de información personal, tanto por parte de organismos públicos -incluyendo la publicación derivada de competencias propias de organismos encargados de las publicaciones oficiales-, como de privados, destacándose a continuación algunas de las decisiones al respecto.

PUBLICACIÓN EN INTERNET DE INFORMACIÓN PERSONAL EN GENERAL

Por Dictamen Nº 17/016, de 14 de setiembre, el Consejo Ejecutivo evaluó una alegada aplicación del denominado "derecho al olvido", conforme lo planteado por la consultante. El Consejo Ejecutivo evaluó que en los casos de publicaciones de informaciones erróneas, inexactas o falsas, corresponde el ejercicio del derecho de supresión ante el editor de las páginas web. Asimismo, resulta trascendente evaluar también la existencia de otros derechos, como la libertad de expresión y prensa, que ameritan una adecuada ponderación con el derecho a la protección de datos personales. En consecuencia, se dictaminó que en la situación planteada el titular de los datos incluidos en publicaciones en internet podría ejercer el derecho de supresión (artículo 15 de la ley) ante el editor de las páginas web y en caso de incumplimiento podrá iniciar la acción judicial de *habeas data* o las administrativas correspondientes ante la unidad.

PUBLICACIÓN EN INTERNET POR PARTE DE ORGANISMOS PÚBLICOS

El Consejo Ejecutivo, en Dictamen Nº 3/016, de 2 de marzo, entendió que la publicación en la página web del organismo consultante de información vinculada al gobierno de facto depende de una adecuada ponderación de los derechos vinculados a la protección de datos personales, acceso a la información pública y derecho a la verdad, correspondiendo, en consecuencia, la elaboración de criterios objetivos para su aplicación a los casos concretos con la participación de todos los organismos involucrados (entre ellos, la Unidad de Acceso a la Información Pública).

Por Resolución Nº 6/016, de 9 de marzo, el Consejo Ejecutivo evaluó la existencia de información personal del denunciante en actas del organismo denunciado -publicadas por mandato legal-, remitiéndose a lo oportunamente establecido en Dictamen Nº 16/012, de 9 de agosto de 2012, indicando que el denunciado posee atribuciones para retirar todo o parte de la versión incorporada al sitio web cuando advierta que este tipo de difusión afecta algún valor esencial o un derecho fundamental.

Por Resolución Nº 54/016, de 8 de setiembre, el Consejo Ejecutivo resolvió recomendar la aplicación de los criterios definidos en la Resolución Nº 1.040/012 y su Anexo para la publicación en la web de información de organismos públicos que contengan datos personales. Ello sin perjuicio de que en el caso concreto los datos mencionados por la denunciante y que se encontraban publicados en la página web del organismo denunciado se encontraban dentro de los exceptuados del previo consentimiento por el artículo 9º literal C) de la ley.

PUBLICACIÓN EN INTERNET DE INFORMACIÓN A TRAVÉS DE ORGANISMOS ENCARGADOS DE PUBLICACIONES OFICIALES

En sentido similar a la Resolución Nº 54/016 se pronunció el Consejo Ejecutivo en el Dictamen Nº 21/016, de 29 de diciembre, recomendando emplear herramientas técnicas para minimizar potenciales vulneraciones a las personas en la protección de sus datos personales frente al efecto expansivo de internet y el rol de los motores de búsqueda, considerando, además, el tipo de información, la pertinencia de su mantenimiento y la afectación a los derechos de los involucrados. Esta consideración corresponde en el caso al organismo consultante (Diario Oficial).

03

AVANCES NORMATIVOS

Desde el punto de vista normativo, en 2016 se produjo la aprobación de las siguientes disposiciones normativas:

3.1 NORMATIVA INTERNACIONAL

Reglamento General de Protección de Datos

El 27 de abril de 2016 se aprobó el Reglamento (General de Protección de Datos) número 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogándose la Directiva 95/46/CE.

Este reglamento, de carácter vinculante para los países miembros de la Unión Europea y que se espera entre en vigencia el 25 de mayo de 2018, trae consigo importantes innovaciones en materia de protección de datos personales, entre las que se destacan el consentimiento, obligaciones para responsables y encargados de tratamiento, transferencias internacionales de datos y cooperación internacional, que serán objeto de análisis por parte de la unidad en el correr del año 2017.

El texto del reglamento puede consultarse en el Diario Oficial de la Unión Europea (http://eur-lex.europa.eu).

Decisión de adecuación *Privacy Shield*

Por su relevancia en lo que respecta a las transferencias internacionales de datos desde la Unión Europea hacia Estados Unidos, entre las normas internacionales de interés se cita la decisión de ejecución (UE) 2016/1250 de la Comisión Europea, de 12 de julio de 2016, sobre la adecuación de la protección conferida por el Escudo de Privacidad UE - EE.UU.

Esta decisión es aplicable en nuestro país conforme lo establecido por la Resolución Nº 17/009, de 12 de junio de 2009.

Puede encontrarse la decisión completa en la página http://eur-lex.europa.eu, con la referencia al número de decisión.

3.2 INFORME SOBRE AVANCES NORMATIVOS

Se presenta a continuación el informe preliminar sobre los aspectos más relevantes del nuevo Reglamento General de Protección de Datos, elaborado por la Dra. Bárbara Muracciole.

Montevideo, 26 de agosto de 2016

INFORME N° 176

BREVE RESEÑA SOBRE EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Con fecha 27 de abril de 2016, el Parlamento Europeo y el Consejo aprobaron el Reglamento Europeo Nº 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, denominado como Reglamento General de Protección de Datos (GDPR por sus siglas en inglés).

Se trata de una norma de aplicación directa en todos los estados miembros de la Unión Europea a partir del 25 de mayo de 2018, sin necesidad de ley que la internalice. Su aprobación, implica la adopción de una legislación única en materia de protección de datos que sustituirá sistemas disímiles ya existentes, nacidos a la luz de la emblemática Directiva 95/46/CE, la cual deroga.

Según expresa el Considerando 9 del Reglamento: *"Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal, en lo que respecta al tratamiento de dichos datos en los Estados miembros pueden impedir la libre circulación de los datos de carácter personal de la Unión. Estas diferencias pueden constituir, por tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan funciones que les incumban en virtud del derecho de la Unión. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE".*

Se estructura en 173 Considerandos, XI Capítulos y 99 artículos, según el siguiente detalle: I) Disposiciones Generales, II) Principios, III) Derechos del Interesado, IV) Responsable de tratamiento y encargado de tratamiento, V) Transferencias de datos personales a terceros países u organizaciones internacionales, VI) Autoridades de control independientes, VII) Cooperación y coherencia, VIII) Recursos, responsabilidad y sanciones, IX) Disposiciones relativas a situaciones específicas de tratamiento, X) Actos delegados y actos de ejecución y XI)Disposiciones finales.

Su objeto, radica en la protección de los derechos y libertades de las personas físicas y, en particular, su derecho a la protección de datos personales.

En cuanto a su ámbito de aplicación material, se aplica al tratamiento total o parcialmente automatizado y no automatizado de datos personales.

Respecto del ámbito territorial, se aplica al tratamiento de datos personales, independientemente que tenga lugar o no en la Unión.

I. GENERALIDADES

En cuanto a las definiciones, este texto amplía e incorpora conceptos respecto a la Directiva 95/46/CE, particularmente con la inclusión -tanto dentro de la definición de dato personal, cuanto como categoría específica- de datos biométricos genéticos y de salud.

Otro aporte relevante lo constituye la definición del consentimiento, que parece inclinarse ante la tesis del consentimiento expreso, al requerir que la manifestación sea inequívoca mediante declaración o acciones expresas.

Destaca, asimismo, la inclusión de la seudonimización como técnica de disociación y del perfilamiento, entendido como *"toda forma de tratamiento automatizado de datos personales consistentes en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física".*

Corresponde mencionar, del mismo modo, la definición de violación de la seguridad como categoría autónoma, lo que demuestra la importancia del tema para esta nueva norma.

En relación con los principios, resalta la previsión del consentimiento de los niños. En este sentido, el legislador europeo dispone que el consentimiento prestado por niños en el marco de ofertas directas de servicios de la sociedad de la información será lícito, cuando el interesado tenga como mínimo 16 años. Si el niño es menor, tal tratamiento se considera lícito si el consentimiento lo prestó o autorizó el titular de la patria potestad o tutela, únicamente en la medida en que se prestó o autorizó. Agrega que los Estados miembros podrán establecer por ley una edad inferior a tales efectos, siempre que no sea menor a 13 años, recayendo sobre el responsable la verificación de los permisos requeridos, habida cuenta la tecnología disponible.

II. NOVEDADES LEGISLATIVAS

1. Derecho de supresión (el derecho al olvido)

El Reglamento legisla expresamente en torno al derecho al olvido en cuanto ejercicio del derecho de supresión. Así, el numeral 1 del artículo 17 dispone que el interesado tendrá derecho, sin dilación indebida del responsable de tratamiento, a la supresión de los datos personales que le conciernan cuando:

- los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
- el interesado retire el consentimiento en que se basa el tratamiento y éste no se apoye en ningún otro concepto jurídico;
- el tratamiento se base en mercadotecnia directa, incluida la elaboración de perfiles relacionada con ésta y no exista otro fundamento jurídico;
- los datos personales hayan sido tratados ilícitamente;
- los datos personales deban suprimirse para cumplir con una obligación legal;

- los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a niños.

Por su parte, el numeral 2 establece que cuando el responsable del tratamiento haya hecho públicos los datos y esté obligado a suprimirlos de acuerdo al numeral 1, teniendo en cuenta la tecnología disponible y el costo de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

Finalmente, el tercer numeral enuncia los casos frente a los cuales no procede el derecho al olvido, debido a que el tratamiento se considera necesario:

- para ejercer el derecho a la libertad de expresión e información;
- para el cumplimiento de una obligación legal que requiere el tratamiento de datos o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
- por razones de interés público en el ámbito de la salud pública;
- con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos,
- para la formulación, el ejercicio o la defensa de reclamaciones.

2. Derecho a la portabilidad de los datos

El artículo 20 del Reglamento, dispone que el interesado tendrá derecho a recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable de tratamiento sin que lo impida el responsable al cual se lo hubiere facilitado, en los casos en que el tratamiento se base en el consentimiento (artículos 6.1 y 9.2) o en un contrato (artículo 6.1) y se efectúe por medios automatizados. La norma aclara que el interesado tendrá derecho a que se sus datos se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. Protección de datos desde el diseño y por defecto

El artículo 25 dispone que el responsable de tratamiento, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, tomando en cuenta el estado de la técnica, el costo de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas, aplicará *"medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir con los requisitos del presente Reglamento y proteger los derechos de los interesados".*

Asimismo, enfatiza que el responsable del tratamiento aplicará las medidas técnicas y organizativas con miras a garantizar que por defecto, sólo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos establecidos, obligación que se aplicará a la cantidad

de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad, para garantizar que los datos personales no sean accesibles sin la intervención del interesado, a un número indeterminado de personas.

Ambos extremos podrán demostrarse mediante procesos de certificación, otra incorporación del Reglamento en su artículo 42, que refiere a que los estados miembros y las autoridades de Control, el Comité y la Comisión, promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos, a fin de demostrar el cumplimiento de lo dispuesto en el Reglamento en las operaciones de tratamiento de los responsables y encargados, teniendo en cuenta las necesidades específicas de las micro empresas y las pequeñas y medianas empresas.

La certificación será voluntaria y se realizará por organismos que deberán cumplir la norma EN ISO/IEC 17065/2012 y requisitos adicionales establecidos por la autoridad de control competente.

4. Registro de actividades de tratamiento

El reglamento elimina el requisito de inscripción y notificación de actividades de tratamiento y lo sustituye por la obligación de cada responsable de llevar un registro de sus actividades, continente de nombre y datos de contacto del responsable, co-responsable, representante y delegado de protección de datos; fines del tratamiento; descripción de las categorías de interesados y datos personales; destinatarios, transferencias internacionales a terceros países u organizaciones internacionales, plazos para la supresión, descripción de medidas técnicas y de seguridad. Por su parte, cada encargado llevará un registro de todas las actividades de tratamiento efectuadas por cuenta del responsable. Tanto el encargado cuanto el responsable, pondrán a disposición el registro cuando lo solicite la autoridad correspondiente.

Estas obligaciones no se aplicarán a empresas ni organizaciones que empleen menos de 250 personas, a menos que el tratamiento entrañe riesgos para los derechos y libertades y no sea ocasional, se trate de datos sensibles o relativos a condenas o infracciones penales.

5. Seguridad del tratamiento

El artículo 32 regula la seguridad del tratamiento y establece que teniendo en cuenta el estado de la técnica, los costos de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos, el responsable y el encargado de tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluya entre otros:

- la seudonimización y el cifrado de datos personales;
- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; y
- la capacidad de restaurar la disponibilidad y acceso a los datos personales de forma rápida en caso de incidentes físicos o técnicos.

La norma exige notificación a la autoridad de control en caso de violación de seguridad y al titular, en caso que entrañe riesgos a los derechos y libertades.

6. Evaluación de impacto relativa a la protección de datos

El artículo 35 prevé un análisis previo del tratamiento para medir su impacto en los derechos y libertades. La norma expresa, que si un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, contexto o fines, es probable que entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable realizará, antes del tratamiento, una evaluación del impacto a cuyos efectos recabará el asesoramiento del delegado de protección de datos. La autoridad de control establecerá y publicará la lista de los tipos de operaciones que requieren esta evaluación de impacto, así como las operaciones que no lo necesitan.

Esta evaluación se requerirá preceptivamente en casos de: a) valoración sistemática y exhaustiva de aspectos personales en forma automatizada, tal como el perfilamiento; b) tratamiento a gran escala de datos sensibles o relativos a condenas e infracciones; y c) observación sistemática a gran escala de una zona de acceso público. Deberá contener, como mínimo, la descripción sistemática de las operaciones de tratamiento previstas y de los fines, inclusive cuando proceda el interés legítimo; la evaluación de la necesidad y la proporcionalidad de las operaciones respecto de su finalidad, y las medidas previstas para afrontar los riesgos.

En los casos en que la evaluación de impacto arroje alto riesgo para los derechos y libertades, el responsable deberá consultar a la autoridad de control.

7. Delegado de Protección de Datos

El artículo 37 erige en forma obligatoria la designación de un delegado de protección de datos en los siguientes supuestos:

- tratamiento llevado a cabo por una autoridad u organismo público, excepto el Poder Judicial en el ejercicio de la función jurisdiccional;
- actividades de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala; y
- tratamiento a gran escala de datos sensibles o relativos a condenas e infracciones penales.

La norma dispone que el delegado *"... será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y a la práctica en materia de protección de datos"*, pudiendo formar parte de la plantilla del responsable o desempeñar sus funciones en el marco de un contrato de servicios. En cualquier caso, el responsable y encargado publicarán su nombre y lo comunicarán a la autoridad de control que corresponda.

El artículo 38 regula la participación del delegado en forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales, garantizando su trabajo e independencia. Será el canal de comunicación a la interna de la institución y entre los titulares y ella, debiendo rendir cuentas al más alto nivel jerárquico. Sus funciones consisten en informar y

asesorar; supervisar el cumplimiento de las normas de protección de datos; ofrecer asesoramiento relativo a la evaluación de impacto; cooperar con la autoridad de control y actuar como punto de contacto con la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, así como formular cualquier otra consulta pertinente.

III. IMPACTO EN URUGUAY

Como señala María Verónica Pérez Asinari, "[d]entro] de las reformas que presenta el nuevo reglamento hay dos aspectos que tienen un impacto directo en Uruguay: a) la adecuación para la transferencia internacional de datos personales y b) la nueva delimitación del ámbito de aplicación territorial, así como su dimensión extraterritorial".[1]

Relacionado con la adecuación, el impacto se debe a que el Reglamento exige a la Comisión Europea revisiones periódicas, al menos cada cuatro años, que tengan en cuenta los desarrollos producidos en los países declarados adecuados.

Es por ello que los países que quieran conservar la adecuación deberán asegurarse que el nivel de protección continúe siendo satisfactorio y que sea acorde a los desarrollos "esenciales" de la materia en la UE. De ese modo, se deberá considerar el impacto de la adopción de la Carta de Derechos Fundamentales y del nuevo reglamento, así como la jurisprudencia europea; tal es el caso Schrems, en el cual la Corte de Justicia de la Unión Europea refuerza el concepto de adecuación al requerir que el nivel de protección sea "esencialmente adecuado".[2]

Respecto al ámbito de aplicación territorial, en función a que el Reglamento se aplicará a las organizaciones y empresas que se encuentren establecidas en el territorio de la Unión y a las que no se encuentren establecidas en su territorio, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a individuos de la Unión, independientemente de si se cobran o no, así como al control de su comportamiento, en la medida que éste tenga lugar en territorio de la Unión.

Es por ello que una empresa uruguaya (por ejemplo, una app o un sitio web) que ofrezca bienes o servicios a individuos en la UE o que controle su comportamiento, deberá cumplir con el nuevo Reglamento de Protección de Datos. Y esto no solo implica cumplir con las obligaciones y respetar los derechos de los individuos, sino también designar un representante en la UE, salvo que la actividad de tratamiento de datos personales sea ocasional.[3]

Dra. Bárbara Muracciole
Derechos Ciudadanos

---

1 *Pérez Asinari, V: "Impacto en Uruguay del nuevo Reglamento de la Unión Europea sobre Protección de Datos Personales", Unidad Reguladora y de Control de Datos Personales, Montevideo 2016, pág. 1. Disponible en internet: www.datospersonales.gub.uy (Fecha de última consulta: 26 de agosto de 2016).*

2 *Ibídem, pág. 3*

3 *Ídem.*

04

INFORMES DE INTERÉS

Se presenta aquí el informe realizado en 2016, firmado por el Dr. Ramiro Prieto, en el entendido que reviste la mayor relevancia desde diferentes puntos de vista relacionados con el derecho a la protección de datos personales.

INFORME VINCULADO CON LA IMPLEMENTACIÓN DE UN SOFTWARE DE REGISTRO ÚNICO DE USUARIOS CON VIH

INFORME N° 62

A. ENCUADRE DEL ASUNTO

Viene a conocimiento de este informante la consulta realizada por la División Epidemiologia del Ministerio de Salud Pública (MSP) con referencia a la implementación de un software de registro único de usuarios de VIH.

El documento elaborado por dicha división, al contextualizar las características del sistema, señala: *"[...] Las características de la epidemia de infección por VIH/SIDA se han modificado con el transcurso del tiempo, pasando a ser un evento transmisible, pero de comportamiento crónico. La generalización del tratamiento antirretroviral (TAR), el inicio del tratamiento en la etapa no sida de la infección, el mayor acceso a programas de prevención de la transmisión materno infantil y a servicios de consejería y pruebas voluntarias, han permitido incrementar el número de personas que realizan la prueba del VIH, y obtener diagnósticos más tempranos en la historia natural de la infección. En este contexto, la vigilancia se ha transformado en un gran desafío para los países. La información necesaria hoy en día, para la implementación de políticas públicas, excede ampliamente los datos que habitualmente se recogen en un sistema de vigilancia convencional [...]"*

Asimismo, el propio documento, con referencia a las características del sistema indica: *"[...] Se trata un sistema web que vincula la información, clínica, epidemiológica y de laboratorio.*

Como se muestra en la siguiente figura las entradas del sistema son:

1. Departamento de Laboratorio de Salud Pública, dado que centraliza los resultados confirmatorios de todo el país.

2. Laboratorios de análisis clínicos que realizan carga viral y CD4. Del relevamiento inicial estos laboratorios son 8 para todo el país. Se pretende contar con un sistema que capture la información registrada en los diferentes sistemas de registro de estos laboratorios. La carga se propone mensual y automatizada. En este sentido los laboratorios como integrantes de este sistema han propuesto acceder a los resultados de estos dos estudios realizados previamente a cada paciente. Esto implica la necesidad de otorgar un permiso para visualizar el módulo de laboratorio del sistema.

3. Los clínicos a cargo de la asistencia institucional de los pacientes VIH. En este punto se pretende contar con un listado definido por las Direcciones Técnicas de los prestadores de salud, de los clínicos que en su institución se dedican a la atención de los pacientes VIH y que por lo tanto podrán acceder en el momento de la atención, a la información ingresada en cualquiera de los módulos del sistema, del paciente que está asistiendo.

Estos permisos deben de estar enmarcados en la base de la confidencialidad y la protección de los datos personales.

Los clínicos tendrán la posibilidad de emitir un resumen de los aspectos más relevantes de la historia del paciente y la obligación de ingresar la información epidemiológica y clínica. En la actualidad estas funciones se realizan a través de formularios en formato papel y de la historia clínica convencional. [...]"

B. ACERCA DEL TRATAMIENTO DE LOS DATOS DE SALUD EN LA LEY N° 18.331

La Ley Nº 18.331 de Protección de Datos Personales y Habeas Data de fecha 11 de agosto de 2008, define a los datos sensibles en su art. 4 Lit. E), indicando que son aquellos: *[...]" datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual [...]"*

Asimismo, el Capítulo IV de la propia Ley (arts. 18 a 23), regula los datos especialmente protegidos, y allí el art 18 prevé la regulación general de los datos sensibles, consagrando específicamente en el art. 19 a los datos de salud.

En dicho marco, el artículo 18 señala: *"[...] Ninguna persona puede ser obligada a proporcionar datos sensibles. Estos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular.*

Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares. [...]"

Por otra parte el art. 19 al regular los datos relativos a la salud indica: *"[...] Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley [...]"*

Lo expuesto, deja de manifiesto el carácter de dato sensible que el legislador consagró para los datos de salud y las garantías especiales de las cuales están revestidos. Por tal motivo, entendemos pertinente analizar los caracteres de su comunicación situación que desde el enfoque de la protección de datos emerge como elemento central de análisis.

C. ACERCA DE LA COMUNICACIÓN DE DATOS DE SALUD Y DE LA PERTINENCIA O NO DE SU DISOCIACIÓN SEGÚN LO DISPUESTO POR EL ART.17 LIT C) DE LA LEY N° 18.331

Si bien analizaremos más adelante las implicancias que cada comunicación de datos producida en el sistema conlleva, creemos pertinente mencionar algunos conceptos que la regulan, con la intención de graficar cuales son las previsiones que al respecto ha identificado el legislador.

En este caso, la comunicación de datos personales de datos de salud, se produce con motivo de la carga de la información del paciente en el sistema, y el posterior acceso a la misma por parte de los actores que participan en el mismo.

La comunicación de datos personales se encuentra regulada en el art. 17 de la Ley Nº 18.331, el cual exige que la misma, deba ser precedida de interés legítimo del emisor y del destinatario de los datos, sin perjuicio del previo consentimiento del titular de los mismos.

Respecto a esta solicitud de consentimiento, el propio art. 17 consagra en sus literales A) a D) aquellas hipótesis en las cuales el mismo resultará exceptuado.

El Lit. C), que fuere actualizado por el artículo 153 de la Ley Nº 18.719 de fecha 27 de diciembre de 2010, prevé la excepción a la solicitud de consentimiento para los datos de salud cuando: *"[...] se trate de datos personales relativos a la salud y sea necesaria su comunicación por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de los titulares de los datos mediante mecanismos de disociación adecuados cuando ello sea pertinente. [...]"*

Como puede apreciarse en el referido literal, el legislador ha previsto la excepción al consentimiento al momento de la comunicación de los datos, pero ha indicado la necesidad de preservar la identidad de sus titulares a través de la disociación de los mismos cuando esto sea pertinente.

Con respecto a la pertinencia, entendemos que la misma debe ponderarse a partir de la existencia de normas jurídicas que regulen el punto que convoca al proyecto y del interés general a las que ellas responden.

En este escenario, es menester tener presente lo dispuesto el artículo 44 de la Constitución Uruguaya el cual dispone: *"[...] El Estado legislará en todas las cuestiones relacionadas con la salud e higiene públicas, procurando el perfeccionamiento físico, moral y social de todos los habitantes del país.*

Todos los habitantes tienen el deber de cuidar su salud, así como el de asistirse en caso de enfermedad. El Estado proporcionará gratuitamente los medios de prevención y de asistencia tan sólo a los indigentes o carentes de recursos suficientes. [...]"

Por otra parte, debemos tener presente lo dispuesto por la Ley Nº 18.335 de fecha 15 de agosto de 2008, la cual en su artículo 22 dispone: *"[...] Toda persona tiene el deber de cuidar de su salud, así como el de asistirse en caso de enfermedad, tal como lo establece el artículo 44 de la Constitución de la República. Asimismo tiene la obligación de someterse a las medidas preventivas o terapéuticas que se le impongan, cuando su estado de salud, a juicio del Ministerio de Salud Pública, pueda constituir un peligro público, tal como lo dispone el artículo 224 del Código Penal.*

El paciente tiene la obligación de suministrar al equipo de salud actuante información cierta, precisa y completa de su proceso de enfermedad, así como de los hábitos de vida adoptados. [...]"

En esta línea y especialmente refiriendo a la enfermedad, diagnostico y tratamiento del VIH, cabe referir también a lo dispuesto por el Decreto N° 409/993 de fecha 23 de setiembre de 1993, el cual en su artículo 1, en la redacción dada por el Decreto Nº 255/008, crea la Comisión Nacional de Lucha Contra el SIDA (CONASIDA) y al regular sus competencias, dispone:

"[...] a) Constituirse en Consejo Consultivo de Coordinación, presentación de propuestas e incidencia en las Políticas Públicas elaboradas y aprobadas por el MSP,

respecto al VIH/SIDA en el marco del acceso universal a la atención integral, trabajando en términos de prevención, asistencia y apoyo a las personas que viven con VIH-SIDA.

b) Proponer y colaborar en la ejecución de actividades sistemáticas, a realizar en conjunto con las instituciones involucradas, que potencien la respuesta nacional ante el VIH/SIDA.

c) Promover la participación directa de representantes de organizaciones especializadas y con trayectoria en VIH/SIDA.

d) Promover la participación directa de representantes de las organizaciones de personas con VIH. [...]"

Por último, y no menos trascendente, debemos tener en cuenta aquellas disposiciones internacionales que han tratado el tema que nos convoca, las cuales han sido ratificadas e incorporadas al ordenamiento jurídico uruguayo y son referidas en el propio Decreto Nº 255/008 de fecha 03 de junio de 2008: *"[...] que existen declaraciones, reglas y directrices en las que son consideradas las normativas de referencia internacional, tales como: a)Leyes especiales que se integraron del Derecho Internacional al Derecho positivo uruguayo, como la Ley Nº 15.737 del 8 de marzo de 1985 de la Convención Americana de Derechos Humanos, Ley Nº 16.137 de 28 de septiembre de 1990 sobre Derechos del Niño, Ley Nº 15.164 del 4 de agosto de 1981 surgida de la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer, Ley Nº 17.338 de 18 de mayo de 2001, referida al Protocolo Facultativo de la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer de 1981; b) Declaraciones: Declaración Universal de los Derechos Humanos, Declaración de Derechos Humanos y la Carta sobre el VIH y el SIDA de 1992, Declaración de los derechos fundamentales de la persona que vive con el VIH/SIDA (Conferencia de Montreal de 1988), Programa Conjunto de las Naciones Unidas sobre el VIH/SIDA (ONUSIDA), Prioridades para la acción en VIH/SIDA en la República Oriental del Uruguay de mayo 2004, fijadas por el Grupo Temático de ONUSIDA en Uruguay, Programa de Acción de la Conferencia Internacional sobre la Población y el Desarrollo de El Cairo en 1994, Programa de Acción de la Conferencia Internacional sobre la Población y el Desarrollo de Beijing en 1995, Revisión del Programa de Acción de la Conferencia Internacional sobre la Población y el Desarrollo de El Cairo en 1994 (CIPD +5), 1999, Revisión del Programa de Acción de la Conferencia Internacional sobre la Población y el Desarrollo de Beijing de 1995 (Beijing +10), 2005; c) Reglas y Directrices: Declaración de Compromiso en la Lucha contra el VIH/SIDA de la Sesión Extraordinaria de la Asamblea General de las Naciones Unidas (UNGASS), 25 a 27 de junio de 2001 y las subsiguientes incluida la de 2006, el VIH/SIDA y los Derechos Humanos, Directrices Internacionales, Segunda Consulta Internacional sobre el VIH/SIDA y los Derechos Humanos de Ginebra 23 a 25 de septiembre de 1996, Naciones Unidas, Nueva York y Ginebra de 1998 [...]"*

En este marco descripto, entendemos que la ponderación exigida por el Lit. C) de la Ley 18.331 (en este caso, a cargo del Ministerio de Salud Pública al diagramar el sistema y sus características, específicamente, la necesidad de recibir la información identificando a su titular, o sea, sin disociarla), responde y se justifica en razón de la normativa antes referida, sin perjuicio de estar directamente relacionado al objetivo que persigue alcanzar el sistema, como instrumento de vigilancia, tratamiento y prevención del VIH y su propagación en el país.

Por último, cabe señalar que esta Unidad se ha expedido en cuestión similar, respondiendo al mismo criterio en Dictamen Nº 18/2010 de fecha 20 de agosto de 2010 con referencia a la improcedencia de la disociación solicitada por el Lit. C) del Art. 17 de la Ley Nº 18.331, ante la preeminencia de legislación especial en la materia. El considerando V) del referido Dictamen señala: *"[...] Que la Historia Clínica posee un régimen jurídico particular, que encuentra fundamento en una ley especial de interés general y de fecha posterior a la que rige la materia tutelada por esta Unidad, como es la Ley Nº 18.335, lo que hace inaplicable el requisito de disociación dispuesto por el art. 17 inc. 3 lit. C) de la Ley Nº 18.331, y habilita a prescindir del consentimiento del titular de los datos, al tenor lo dispuesto por el inc. A del mismo artículo ante citado [...]"*

Por lo tanto y en función de lo expuesto, entendemos que la decisión del Ministerio de Salud Publica de que los participantes en el sistema comuniquen la información del paciente sin disociar, es legítima, ya que responde a la necesidad de dar cumplimiento a un marco normativo general y no se aparta de las previsiones de la Ley Nº 18.331.

D. ACERCA DE LA LEGALIDAD EN EL TRATAMIENTO DE DATOS PERSONALES POR PARTE DE LOS SUJETOS Y ENTIDADES QUE PARTICIPAN EN EL SISTEMA

Analizado el régimen aplicable a los datos de salud, como datos especialmente protegidos a los que el legislador en la Ley Nº 18.331 dotó de garantías especiales y las exigencias previstas por la propia norma para la comunicación de los mismos, con especial referencia a la necesidad de disociación de los mismos, nos corresponde abordar el análisis de la viabilidad jurídica del proyecto que nos convoca, identificando el impacto que este podría acarrear desde la óptica de la Protección de Datos Personales y su legislación vigente.

A tales efectos, creemos oportuno, diferenciar el rol de cada uno de los actores que participan en las distintas instancias previstas en la plataforma, para analizar la legitimidad de su actuación y del tratamiento de los datos personales de los pacientes.

D.1. EL MINISTERIO DE SALUD PÚBLICA

En primera instancia, nos corresponde analizar la situación del Ministerio de Salud Pública (MSP) y sus dependencias, con respecto del sistema a implementarse.

A estos efectos, entendemos mas ilustrativo, abordar por separado cada una de las cuestiones del proyecto que le atienen.

D.1.a. Acerca del Ministerio de Salud Pública como titular de la base de datos

La División de Epidemiologia- Departamento de Vigilancia en Salud, del Ministerio de Salud Publica, es quien impulsa el proyecto de estudio y quien será titular de la base de datos generada.

En este marco, nos corresponde referir al documento que describe el proyecto, el cual identifica la necesidad de actualizar los instrumentos de vigilancia elaborados por el Departamento de Vigilancia en Salud (DEVISA) (res-

ponsable de la vigilancia de este evento, y el programa de ITS/Sida) el cual señala: *"[...]Por otro lado, se identifican fortalezas que deben considerase al momento de definir una modificación en el sistema de vigilancia y que nos indican que existen condiciones favorables para que una propuesta sea viable. En primer lugar en nuestro país existe un solo laboratorio (Departamento de Laboratorios de Salud Pública) que realiza el test confirmatorio de VIH, por lo que los casos están todos centralizados, X laboratorios que realizan carga viral y recuento de CD4, centros de atención de referencia para adultos (SEIC) y para niños (CHPR) que concentran la atención de gran número de infectados y un número limitado de profesionales dedicados a la asistencia de estos pacientes.*

Como un hecho no menor, las autoridades de las diferentes áreas involucradas, entienden como necesario el desarrollo de nuevas estrategias y la adaptación del sistema de vigilancia a los nuevos conceptos de vigilancia, monitoreo y evaluación. Por este motivo se plantea introducir en la vigilancia el concepto de proceso longitudinal, que incluya desde el inicio de la infección, hasta el fallecimiento, con indicadores intermedios, que permitan continuar describiendo la epidemia, pero además monitorizar y evaluar el impacto de las intervenciones, así como identificar necesidades prioritarias, para una correcta distribución de los recursos y de las medidas, tendiendo a la equidad de los servicios. [...]"

En este marco en que el Ministerio de Salud Publica, (a través del Programa ITS/SIDA y del Departamento de Vigilancia en Salud), será titular de la base de datos que se impulsa con el proyecto, cabe tener presente el rol de tal Ministerio, como órgano integrante del sistema orgánico Poder Ejecutivo, en ejercicio de los cometidos referentes a la sanidad nacional.

Al respecto, el art. 1 de la Ley Orgánica de Salud Publica, Ley Nº 9202 de fecha 12 de enero de 1934, dispone: *"[...] Compete al Poder Ejecutivo por intermedio de su Ministerio de Salud Publica, la organización y dirección de los servicios de Asistencia e Higiene. En materia administrativa, el Ministerio de Salud Pública se regirá por lo dispuesto en esta Ley y en el Decreto Orgánico de los Ministerios, en cuanto fuera aplicable. [...]"*

Por tanto, entendemos que la legalidad de la titularidad de la base de datos por parte del Ministerio de Salud Publica resulta incuestionable.

D.1.b. Acerca del rol del Ministerio de Salud Pública en la implementación del sistema

En segundo lugar, nos corresponde determinar el rol y las funciones que desempeñará el referido Ministerio en el sistema que motiva esta consulta.

En este caso, el documento del proyecto señala: *"[...] El Ministerio de Salud Pública a través del Programa ITS/Sida y del Departamento de Vigilancia en Salud accederá a la información sin restricciones y a nivel nacional [...]"*

Tal previsión es lógica, en el entendido de que como se mencionó la titularidad de la base de datos pertenecerá al MSP a través una de sus divisiones con competencia, siendo destinatario y accediendo en cualquier momento a la información comunicada, la cual es cargada por los laboratorios de análisis clínicos y por los profesionales clínicos que participan del tratamiento del paciente.

Esta recepción de la información o datos del paciente, la entendemos legítima en función de lo dispuesto en el art. 18 inc. 2 de la Ley Nº 18.331 que dispone: *"[...] Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares. [...]"*

Con referencia a las razones de interés general y la necesidad de fundamento legal del organismo solicitante de la información, debemos tener presente lo dispuesto por la Ley Nº 18.211 de 13 de diciembre de 2007, la cual regula la creación, funcionamiento y financiación del Sistema Nacional Integrado de Salud (SNIS). El art. 1 de la referida norma dispone: *"[...] La presente ley reglamenta el derecho a la protección de la salud que tienen todos los habitantes residentes en el país y establece las modalidades para su acceso a servicios integrales de salud. Sus disposiciones son de orden público e interés social. [...]"*

Por otra parte el art. 2 establece como competencia del Ministerio de Salud Publica la implementación de dicho sistema y la articulación de los prestadores públicos y privados.

Asimismo, el art. 4 Lit. B al regular los objetivos del SNIS, consagra la implementación de un modelo de atención integral basado en una estrategia sanitaria común, políticas de salud articuladas, programas integrales y acciones de promoción, protección, diagnostico precoz, tratamiento oportuno, recuperación y rehabilitación de la salud de sus usuarios, incluyendo los cuidados paliativos; y el art.4 Lit. C consagra como objetivos: impulsar la descentralización en la ejecución en el marco de la centralización normativa, promoviendo la coordinación entre dependencias nacionales y departamentales. Por otra parte, el Lit. F señala que es objetivo del sistema promover el desarrollo profesional continuo de los recursos humanos para la salud, el trabajo en equipos interdisciplinarios y la investigación científica.

Todo lo indicado, bajo la competencia del Ministerio de Salud Publica como articulador del SNIS por disposición del antes referido art. 2.

Otra disposición relevante para dilucidar el punto de análisis, es el artículo 8 de la propia norma que señala: *"[...] El control de la calidad integral de la atención en salud a cargo del Ministerio de Salud Pública tomará en cuenta el respeto a principios de la bioética y a los derechos humanos de los usuarios.*

Dicha modalidad será aplicable a la incorporación y uso de tecnologías y medicamentos. [...]"

Por otra parte, cabe tener presente que el art. 11 dispone que podrán integrar el SNIS, tanto los servicios de salud a cargo de personas jurídicas públicas estatales y no estatales, y la entidades a que refiere el art. 265 de la ley 17.930 de 19 de diciembre de 2005, (las cuales son las instituciones de asistencia médica colectiva, previstas en el art.6 del Decreto-Ley 15.181, así como las instituciones de asistencia médica privada particular sin fines de lucro y los seguros integrales autorizados y habilitados por el Ministerio de Salud Publica).

En último lugar, debemos hacer mención a que el art. 49 de la norma de análisis dispone que son usuarios del SNIS todas las personas que residan en el territorio nacional y se registren espontáneamente o a solicitud de la Junta Nacional de Salud, en alguna de las entidades prestadoras de servicios de salud

que lo integren, cometiéndose a la reglamentación las condiciones del registro, por lo que integrarán el SNIS aquellos sujetos a los que se les detecte la enfermedad.

En esta línea, no cabe dudas que la información que recepciona el Ministerio de Salud Publica en el marco de un Sistema Nacional Integrado de Salud, como titular de la base de datos de pacientes que padecen VIH y su posterior acceso en cualquier instancia y sin restricciones a través de la división competente, con la única finalidad de aumentar la vigilancia de la enfermedad, mejorar su tratamiento, y fomentar su prevención, se entiende acorde a derecho. Máxime, cuando la enfermedad se ha convertido en crónica y su vigilancia ha pasado a cumplir un rol fundamental en su tratamiento tal como señala la descripción del proyecto *"[...] Las características de la epidemia de infección por VIH/SIDA se han modificado con el transcurso del tiempo, pasando a ser un evento transmisible, pero de comportamiento crónico [...]"*

D.2. LOS LABORATORIOS DE ANÁLISIS CLÍNICOS

Con referencia al rol de estos laboratorios de análisis clínicos el proyecto señala: *"[...]En primer lugar en nuestro país existe un solo laboratorio (Departamento de Laboratorios de Salud Pública) que realiza el test confirmatorio de VIH, por lo que los casos están todos centralizados, X laboratorios que realizan carga viral y recuento de CD4, centros de atención de referencia para adultos (SEIC) y para niños (CHPR) que concentran la atención de gran número de infectados y un número limitado de profesionales dedicados a la asistencia de estos pacientes. [...]"*

Por otra parte, el propio proyecto, también señala con referencia al rol que cumplirán estos laboratorios de análisis clínicos en el sistema lo siguiente: *"[...] Del relevamiento inicial estos laboratorios son 8 para todo el país. Se pretende contar con un sistema que capture la información registrada en los diferentes sistemas de registro de estos laboratorios. La carga se propone mensual y automatizada. En este sentido los laboratorios como integrantes de este sistema han propuesto acceder a los resultados de estos dos estudios realizados previamente a cada paciente. Esto implica la necesidad de otorgar un permiso para visualizar el módulo de laboratorio del sistema. [...]"*

Encuadrado su rol en el sistema, nos corresponde analizar cuál es la legalidad en el tratamiento de datos realizado y determinar la legitimidad de su actuación.

D.2.a. Acerca de la comunicación de datos entre el laboratorio de análisis clínicos y el MSP

Tal cual señalamos, la carga de la información del paciente en el sistema por parte del Laboratorio de análisis clínicos, responde a una hipótesis de comunicación de datos personales, por encuadrar en la definición prevista en el art. 4 Lit. B de la Ley Nº 18.331 el que dispone: *"[...] Comunicación de datos: toda revelación de datos realizada a una persona distinta del titular de los datos [...]"*

En este caso, los datos cargados en la plataforma por los referidos laboratorios tendrán como destinatario al Ministerio de Salud Publica, titular del sistema.

Cabe adelantar, que esta comunicación la entendemos ajustada a derecho por los argumentos que expresaremos a continuación.

Como se mencionó en otras instancias de este informe, la comunicación de datos personales se encuentra regulada en el art. 17 de la Ley Nº 18.331. Este articulo, exige que la misma deba ser precedida de interés legítimo del emisor y del destinatario de los datos, sin perjuicio del previo consentimiento del titular del dato. Respecto a éste, el propio art. 17 consagra en sus literales A) a D) aquellas hipótesis en las cuales el mismo resultará exceptuado.

En primer término, analizaremos el interés legítimo del emisor de los datos (el Laboratorio de análisis clínicos) y del destinatario de los mismos (el Ministerio de Salud Publica).

En este marco, corresponde señalar que la exigencia de interés legítimo prevista por la normativa, responde a la necesidad de que la información o el dato personal comunicado, sea emitido y accesible en virtud de algún fundamento sólido que así lo permita, excluyendo de tal situación a aquel mero interés o interés simple el cual no justificaría difundir ni acceder a tal información por parte del emisor y del destinatario. En este escenario, este interés legitimo, puede responder por ejemplo, a la necesidad de dar cumplimiento a alguna norma jurídica por parte del emisor y el destinatario.

Este interés legitimo, establecido como presupuesto normativo, previo a la comunicación, busca reforzar la protección del dato al momento de ser comunicado, no limitando la posibilidad de su comunicación a la sola existencia del consentimiento previo o en su defecto a la configuración de alguna de sus excepciones.

Por tanto, entendemos que los laboratorios de análisis (ocho en todo el país que revisten las condiciones para prestar el servicio requerido, tal cual señala el proyecto) cargan la información del paciente y la comunican, revistiendo interés legitimo en función de lo dispuesto por el art. 4 Lit. B la Ley Nº 18.211, el cual como señalamos, al regular los objetivos del SNIS, consagra la implementación de un modelo de atención integral basado en una estrategia sanitaria común, políticas de salud articuladas, programas integrales y acciones de promoción, protección, diagnostico precoz, tratamiento oportuno, recuperación y rehabilitación de la salud de sus usuarios, incluyendo los cuidados paliativos.

Por otra parte, cabe recordar que estos Laboratorios de análisis clínicos integran el SNIS en función de lo dispuesto por el art. 11 de dicha norma, al cual también anteriormente hemos referido.

Con referencia al interés legitimo que reviste al Ministerio de Salud Publica en tanto destinatario de los datos del paciente, el mismo queda de manifiesto en función de las normas a las que en otros apartados de este informe hemos referido, más específicamente, por lo dispuesto por el art. 4 de la Ley Orgánica de Salud Publica Nº 9202, en tanto dota a tal órgano del Poder Ejecutivo del cometido de policía sanitaria.

También, se justifica el interés legitimo, en función de lo dispuesto por el art.2 de la Ley Nº 18.211, el cual establece como competencia del Ministerio de Salud Publica la implementación y la articulación de los prestadores públicos y privados en el marco de la creación, funcionamiento y financiación del

Sistema Nacional Integrado de Salud. Normas a la que también hemos referido anteriormente.

Finalmente, nos corresponde analizar la situación del segundo de los presupuestos previstos por el art. 17 de la Ley Nº 18.331, en este caso, el consentimiento informado del paciente previo a esta comunicación de datos.

En dicho marco, entendemos que éste resulta exceptuado por aplicación de los Literales A) B) y C) previstos en el propio artículo.

Entendemos aplicable la excepción a la solicitud de consentimiento prevista en el Lit. A de la Ley 18.331, en virtud de que se exime del mismo cuando: *"[...] así lo disponga una ley de interés general [...]"*. En este marco, entendemos que las disposiciones constitucionales y legales citadas anteriormente en este informe, responden claramente al interés general, por lo que son marco suficiente para que opere la excepción al previo consentimiento prevista.

Con referencia a la aplicación del Lit. B), éste, remite a las excepciones al consentimiento previstas en el art. 9 de la propia Ley y allí entendemos de aplicación al caso, la previsto en el Lit. B), que exceptúa de consentimiento previo a aquellos datos que: *"[...] se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. [...]"*

En este sentido, al Poder Ejecutivo en ejercicio de función administrativa, le corresponde el cometido de policía sanitaria a nivel nacional, el cual ejerce a través del Ministerio de Salud Publica tal cual dispone la Ley Orgánica de la Salud Nº 9202 en su art. 1: *"[...] Compete al Poder Ejecutivo por intermedio de su Ministerio de Salud Publica, la organización y dirección de los servicios de asistencia e higiene. En materia administrativa, el Ministerio de Salud Publica se regirá por lo dispuesto en esta Ley y en el Decreto Orgánico de los Ministerios, en cuanto fuera aplicable [...]"*

Lo señalado no hace más que confirmar la aplicación de la excepción al consentimiento prevista en el art. 9 Lit. B de la Ley Nº 18.331, por remisión del articulo 17 Lit. B.

Asimismo, creemos pertinente considerar que en virtud de la especialidad que revisten los datos de salud a comunicar, y la previsión expresa del legislador para los mismos en el Lit. C) del propio artículo, la excepción al consentimiento aplicable al caso, es la prevista en el art. 17 Lit. C, para cuyo análisis nos corresponde remitirnos a lo analizado en el punto C de este informe.

D.2.b. Acerca del acceso al sistema por parte de los laboratorios de análisis clínicos

Otro aspecto a analizar respecto de los Laboratorios de Análisis Clínicos, es la posibilidad prevista de que estos accedan a algunos datos o información específica del paciente, una vez cargada en el sistema. En este sentido, el proyecto señala: *"[...] La carga se propone mensual y automatizada. En este sentido los laboratorios como integrantes de este sistema han propuesto acceder a los resultados de estos dos estudios realizados previamente a cada paciente. Esto implica la necesidad de otorgar un permiso para visualizar el módulo de laboratorio del sistema. [...]"*

Este tratamiento de datos que opera a partir del acceso al sistema por parte de los laboratorios una vez que hacen la carga de los datos, también lo

entendemos ajustado a derecho ya que entendemos que la misma encuadra en lo previsto en el art. 19 de la Ley Nº 18.331, el cual indica: *"[...] Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley [...]"*

Independientemente de lo referenciado, cabe señalar que la información a la que solicitan acceder los referidos laboratorios, es información que estos ya poseen, puesto que son ellos los que realizan carga viral y recuento de CD4, tal cual luce en el proyecto presentado.

Por tanto, entendemos que en este caso, no habría inconvenientes en el tratamiento de la información que se provoca con el acceso por parte del laboratorio. Sin perjuicio de esto, se deben extremar los cuidados a la hora de proveer los accesos al sistema, a los efectos de garantizar que el propio laboratorio solamente acceda a la información que posee y que responde a su interés, no accediendo a información adicional que pueda implicar una vulneración a los derechos del titular de la información.

E. ACERCA DE LA COMUNICACIÓN DE DATOS DE LOS CLINICOS AL MSP

Por último, nos corresponde abordar la situación de los médicos o clínicos a cargo del tratamiento del paciente en cada uno de los prestadores de salud. Con referencia a la carga de información en el sistema por parte de estos, el proyecto señala: *"[...] Los clínicos a cargo de la asistencia institucional de los pacientes VIH. En este punto se pretende contar con un listado definido por las Direcciones Técnicas de los prestadores de salud, de los clínicos que en su institución se dedican a la atención de los pacientes VIH y que por lo tanto podrán acceder en el momento de la atención, a la información ingresada en cualquiera de los módulos del sistema, del paciente que está asistiendo.*

Estos permisos deben de estar enmarcados en la base de la confidencialidad y la protección de los datos personales.

Los clínicos tendrán la posibilidad de emitir un resumen de los aspectos más relevantes de la historia del paciente y la obligación de ingresar la información epidemiológica y clínica. En la actualidad estas funciones se realizan a través de formularios en formato papel y de la historia clínica convencional. [...]"

En la hipótesis de análisis, nuevamente nos encontramos frente a una hipótesis de comunicación de datos personales, en este caso el clínico comunicará información perteneciente a su paciente al Ministerio de Salud Pública, y a la misma información, en este caso referente a datos de tratamiento del paciente accederán otros médicos, los cuales oportunamente estarán a cargo del paciente.

Con referencia a dicha comunicación de datos, debemos tener presente lo dispuesto en el art. 17 de la Ley Nº 18.331 al que ya hemos referido, y exige que la misma, deba ser precedida de interés legítimo del emisor y del destinatario de los datos, sin perjuicio del previo consentimiento del titular de los mismos.

Con referencia al interés legitimo, entendemos que el mismo es revestido por el emisor, en este caso el médico, el cual debe aportar la información en función del cumplimiento de deberes inherentes a su profesión. Por otra parte, también reviste tal interés el Ministerio de Salud Pública quien ejerce el cometido de policía en materia sanitaria, por mandato de los art. 44 de la Constitución, la Ley Orgánica de la Salud Nº 9202 y la Ley Nº 18.211 de SNIS que lo consagra como el articulador y promotor del sistema.

En segundo lugar, entendemos que no es necesario el previo consentimiento del titular del dato, por operar la excepción prevista en el art. 17 Lit. C), aplicable a los datos de salud, con referencia a la pertinencia de la identificación del titular o más específicamente de la disociación prevista en el propio artículo, cabe remitirnos a lo referido en el punto C de este informe.

Asimismo, entendemos legitimo el tratamiento de datos realizado por el Ministerio de Salud Publica, en virtud de que éste también encuadra en lo previsto en el art. 18 inc.2 de la Ley Nº 18.331 el cual indica: *"[...] Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares. [...]"*

E.1. ACERCA DE LA COMUNICACIÓN DE LA INFORMACIÓN CLINICA DEL PACIENTE POR PARTE DEL MSP A LOS MEDICOS TRATANTES

Otra cuestión que merece nuestro abordaje refiere a los datos del paciente o información clínica cargada en el sistema del MSP, la cual es comunicada o accesible a los médicos o clínicos previamente seleccionados por los prestadores de salud para dar tratamiento al paciente.

Nuevamente, debemos analizar si en el caso, se reúnen los extremos requeridos por el art. 17 de la Ley Nº 18.331 previos para la comunicación de datos.

Con referencia a la necesidad de interés legítimo exigida por dicho artículo, entendemos que el mismo es revestido tanto por el emisor como por el destinatario de los datos. En el caso del MSP, corresponde remitirnos a lo mencionado en el apartado anterior de este informe, no en vano, cabe recordar que esta base de datos tiene por objeto el seguimiento y tratamiento de pacientes que padecen el virus de VIH, por lo que el seguimiento de la evolución de la enfermedad, responde a los cometidos que ejerce el MSP. Por otro lado, desde la óptica del destinatario, o el médico tratante en cuestión, tal información es relevante a los efectos del ejercicio de aquellos deberes que son inherentes al ejercicio de su profesión.

Por otro lado, con respecto al consentimiento previo, entendemos que el mismo resulta exceptuado por aplicación de la excepción prevista en el art. 17 Lit. C de la Ley Nº 18.331. Asimismo, y tal cual mencionamos en el apartado C de este informe, la identificación de los pacientes resulta pertinente y relevante para llevar a cabo el tratamiento y cumplir con la finalidad del sistema.

En el caso de análisis, debemos tener presente lo previsto en el art. 11 de la Ley Nº 18.331. Tal artículo, consagra el principio de reserva señalando: *"[...] Aquellas personas físicas o jurídicas que obtuvieren legítimamente información*

proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros.

Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular.

Esta obligación subsistirá aún después de finalizada la relación con el responsable de la base de datos. [...]"

Respecto a si este principio de reserva obsta o no a los médicos a acceder a la información del paciente, entendemos pertinente hacer una serie de consideraciones.

En primera instancia, entendemos que este art. 11 refiere a la revelación de la información a terceros, entendiéndose por estos a sujetos externos o ajenos al tratamiento, en este caso entendemos que el MSP no será ajeno al mismo, sino que es parte del tratamiento, no desde el punto de vista clínico, pero si desde la óptica administrativa, ya que es el encargado de implementar la política pública y su seguimiento referente al tratamiento de la enfermedad, por aplicación del Decreto N° 409/993 – creación de comisión nacional de lucha contra el sida (CONASIDA), en la redacción dada por el Decreto Nº 255/008, sin perjuicio de lo previsto en el art. 4 lit. B de la Ley 18.211 el cual regula los objetivos del SNIS, los cuales el MSP tiene el deber de implementar.

Esto, sin perjuicio de lo previsto por el art. 1 de la Ley Orgánica de la Salud Nº 9202, la cual pone en manos del Poder Ejecutivo a través de su ministerio de Salud Publica la competencia respecto a la organización y dirección de los servicios de asistencia e higiene, y del art. 3 de la propia norma la cual dispone *"[...] En materia de asistencia, compete al Ministerio de Salud Publica, la organización, administración y funcionamiento de los servicios destinados al cuidado y tratamiento de enfermos y la administración de los establecimientos destinados a la protección de incapaces y menores desamparados, que no quedaren sujetos al Ministerio de Protección de la Infancia [...]"*

Con referencia al segundo inciso del art. 11, en este caso a la obligación de guardar secreto profesional, el mismo cesa para el caso de estudio, en virtud la aplicación de normativa especial, que regula el accionar de los médicos a la hora del ejercicio de su profesión, como lo es la Ley Nº 19.286 o Código de Ética Médica, el cual regula específicamente el punto en su artículo 22.

Este articulo 22, dispone:

"[...]a) El respeto a la confidencialidad es un deber inherente a la profesión médica.

b) Solo podrá ser relevado en los casos establecidos por una ley de interés general o cuando exista justa causa de revelación. Se consideran, por ejemplo, como justa causa de revelación las siguientes:

- Peligro vital inminente para el paciente (por ejemplo riesgo de suicidio).

- Negativa sistemática del paciente de advertir a un tercero acerca de un riesgo grave para la salud de este último (contagio de enfermedades transmisibles, por ejemplo).

- Amenaza concreta para la vida de terceros.

- Defensa legal contra una acusación de un paciente. [...]"

De este artículo, se desprenden las causales válidas para relevar la confidencialidad requerida para el ejercicio de la profesión médica, las cuales se encuentran mencionadas a titulo enunciativo.

En este caso, entendemos aplicables al proyecto de estudio las causales previstas, más específicamente la que prevé: *"[...] Negativa sistemática del paciente de advertir a un tercero acerca de un riesgo grave para la salud de este último (contagio de enfermedades transmisibles, por ejemplo). [...]"*

En virtud de los argumentos expuestos, entendemos que el sistema tampoco vulnera las previsiones del art 11 de la Ley Nº 18.331, ni conlleva responsabilidad alguna para el médico tratante, en función de que la información cargada en el sistema, es incluida y accedida en virtud del tratamiento de la enfermedad de un paciente, sobre el cual el médico debe actuar acorde a los deberes inherentes a su función previstos en la normativa.

Asimismo, cabe tener presente lo señalado en el documento del proyecto en donde se señala: *"[...] Los clínicos tendrán la posibilidad de emitir un resumen de los aspectos más relevantes de la historia del paciente y la obligación de ingresar la información epidemiológica y clínica. En la actualidad estas funciones se realizan a través de formularios en formato papel y de la historia clínica convencional. [...]"*

Con referencia a este último punto, cabe tener presente lo dispuesto en el art. 18 Lit. D) que señala: *"[...] Que se lleve una historia clínica completa, escrita o electrónica, donde figure la evolución de su estado de salud desde el nacimiento hasta la muerte.*

La historia clínica constituye un conjunto de documentos, no sujetos a alteración ni destrucción, salvo lo establecido en la normativa vigente.

El paciente tiene derecho a revisar su historia clínica y a obtener una copia de la misma a sus expensas, y en caso de indigencia le será proporcionada al paciente en forma gratuita.

En caso de que una persona cambie de institución o de sistema de cobertura asistencial, la nueva institución o sistema deberá recabar de la o del de origen la historia clínica completa del usuario. El costo de dicha gestión será de cargo de la institución solicitante y la misma deberá contar previamente con autorización expresa del usuario.

La historia clínica es de propiedad del paciente, será reservada y sólo podrán acceder a la misma los responsables de la atención médica y el personal administrativo

vinculado con éstos, el paciente o en su caso la familia y el Ministerio de Salud Pública cuando lo considere pertinente.

El revelar su contenido, sin que fuere necesario para el tratamiento o mediare orden judicial o conforme con lo dispuesto por el artículo 19 de la presente ley, hará pasible del delito previsto en el artículo 302 del Código Penal [...]"

La información que luce en el sistema responde al tratamiento del paciente, por lo que debe ser cargada de manera completa. Asimismo, tal cual mencionamos anteriormente, entendemos no hay revelación de contenido de la misma a terceros, sino que la información siempre circula dentro del marco de dicho tratamiento.

En último lugar, no debemos olvidar que en función de lo dispuesto por los arts. 44 de la Constitución de la Republica, art. 244 del Código Penal, art. 22 de la Ley Nº 18.335 y art. 4 de la Ley Nº 9202, los habitantes tienen el deber de asistirse sanitariamente, obligación cuyo cumplimiento entendemos no puede estar condicionada a la entrega de la información por parte de un medico participante en el tratamiento.

Sin perjuicio de lo señalado, y si bien el documento que elabora el proyecto hace alusión a la restricción de acceso al mismo por parte de los clínicos pertenecientes a cada institución de asistencia médica, el cual está sujeto al previo listado de profesionales enviados por la misma, corresponde al MSP extremar los cuidados al respecto, a los efectos de que se cumpla lo previsto y solo accedan a la información del paciente los clínicos a cargo de su tratamiento.

F. CONCLUSIONES

Como conclusión a lo expuesto cabe señalar que:

En primer lugar, que el proyecto objeto de esta consulta prevé el tratamiento de datos de salud, los cuales son datos sensibles en virtud de lo dispuesto por el art. 4 de la Ley 18.331.

En segundo lugar, que a los efectos de su comunicación, se debe tener presente lo dispuesto en el art. 17 Lit. C), aplicable específicamente a tales datos de salud, en donde se prevé la excepción al consentimiento al momento de la referida comunicación de datos, pero ha indicado la necesidad de preservar la identidad de sus titulares a través de la disociación de los mismos cuando esto sea pertinente.

En tercer lugar, que se entiende que la decisión del MSP de solicitar que la información sea comunicada sin disociarla de su titular es acorde a derecho, ya que la pertinencia de la misma, debe ponderarse a la luz de las normas jurídicas que regulan el punto objeto de este proyecto y así como el interés general a las que ellas responden, como son los Art. 44 de la Constitución de la República, el art. 22 de la Ley Nº 18.335, así como el Decreto Nº 409/993, en la redacción dada por el Decreto Nº 255/008, así como las disposiciones internacionales ratificados e incorporadas al ordenamiento jurídico uruguayo.

En cuarto lugar, que la titularidad de la base de datos revestida por el MSP se entiende acorde a derecho, en función de que tal Ministerio, en su calidad de órgano integrante del sistema orgánico Poder Ejecutivo, ejerce los

cometidos referentes de sanidad nacional en función de lo dispuesto en el art. 1 de la Ley orgánica de la Salud Nº 9202.

En quinto lugar, que el acceso a la información del sistema, sin restricciones por parte del MSP se entiende legitima, se ajusta a lo dispuesto por el inc. 2 del art. 18 de la Ley Nº 18.331, en virtud de que median razones de interés general por aplicación de lo dispuesto en los arts. 1, 2, 4 Lit. B) ,11 y 49 de la Ley Nº 18.211 que regula el SNIS.

En sexto lugar, que la comunicación de datos realizada por los laboratorios de análisis clínicos al cargar la información del paciente en el sistema se encuentra precedida de el interés legitimo del emisor (laboratorio) y del destinatario (MSP), el cual es revestido por el laboratorio en función de la necesidad de dar cumplimiento a la normativa vigente, como son los arts. 4 Lit. B) y 11 de la Ley Nº 18.211 y por el MSP en función de lo dispuesto en el art. 4 de la Ley Orgánica de la Salud Nº 9202 y el art. 2 de la Ley Nº 18.211. Asimismo, entendemos que no será necesario consentimiento previo por aplicación del art. 17 Lit. C), sin perjuicio de reunirse también las condiciones para la aplicación de las excepciones previstas en el Lit. A) del propio artículo y en el art. 9 Lit. B), por remisión del art. 17 Lit. B).

En séptimo lugar, que la solicitud de acceso a la información que solicitan los propios laboratorios de análisis clínicos, se entiende acorde con lo previsto por el art. 19 de la Ley Nº 18.331, con motivo de que los titulares han sido pacientes de la entidad, por tanto la misma ya posee tal información accediendo en este caso por otra vía. Esto sin perjuicio de que se deben extremar los cuidados para que los referidos laboratorios no accedan a información que excedan el marco de su actuación.

En octavo lugar, que la comunicación de datos que opera con motivo de la comunicación de la información del paciente por parte de los clínicos o médicos tratantes con destino al MSP, esta revestida de interés legítimo para ambas partes. Para los médicos por aplicación del Código de Ética Médica Ley Nº 19.286, y para el ministerio por mandato del art. 44 de la constitución, el art. 1 de La ley Orgánica de la Salud Nº 9202 y el art. 2 de la Ley Nº 18.211. Asimismo, tampoco será necesario el consentimiento del titular por aplicación de la excepción prevista en el art. 17 Lit. C). Sin perjuicio de lo dispuesto en el art. 18 inc. 2, el cual legitima el tratamiento de datos del MSP.

En noveno lugar, que la comunicación de la información médica del paciente por la carga en el sistema del médico tratante y su acceso por parte del MSP y otros médicos tratantes, responde al interés general exigido y al que anteriormente hemos referido, y que por otra parte no requiere consentimiento previo del titular por aplicación de, ya mencionado art. 17 Lit. C), no violenta el principio de reserva previsto en el art. 11 de la Ley Nº 18.331, en virtud de que tal circulación de información se da en el marco del tratamiento y a la misma no acceden terceros ajenos a esta, sin perjuicio de que la confidencialidad que deberá guardar el médico en ocasión de la información recabada en el ejercicio de su profesión, puede ser relevado por aplicación de las casuales previstas en el art. 22 del Código de Ética Médica Ley Nº 19.286, aplicables al caso que nos convoca. Lo indicado, sin perjuicio también, del derecho del paciente previsto en el art. 18 Lit. D) de la Ley Nº 18.335 que prevé se lleve una historia clínica del paciente completa e integra y del deber que estos tienen de asistirse en función de lo previsto por el art. 44 de la Constitución de la Republica, el art.

224 del Código Penal, así como el art. 22 de la Ley Nº 18.335 y el art. 4 de la Ley Nº 9202. Asimismo, se recomienda al MSP extremar los cuidados a la hora de otorgar los permisos y accesos al sistema restringiendo estos solamente a los clínicos que participan en el tratamiento en cada institución médica.

En definitiva, este informante entiende que el sistema propuesto por el Ministerio de Salud Pública, se ajusta a las disposiciones legales y reglamentarias, estando acorde a derecho su implementación.

Dr. Ramiro Prieto Aguiar
Derechos Ciudadanos

05

SENTENCIAS INTERNACIONALES DE INTERÉS

Sin perjuicio de la existencia de una constante y profusa jurisprudencia en la materia, que reviste el máximo interés, se han escogido las sentencias que se indican a continuación en mérito a su relevancia sustantiva para la defensa activa del derecho a la protección de datos personales.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

Caso "Patrick Breyer v. Germany"

El caso trata de la recolección de direcciones IP de visitantes a las páginas del gobierno alemán. El denunciante afirmó ante el tribunal que las direcciones IP son datos personales bajo la normativa de la Unión Europea y que, en consecuencia, se requería consentimiento para el tratamiento de esos datos y para la potencial elaboración de perfiles.

No se discute en el caso la diferencia entre direcciones IP estáticas y dinámicas, ya que la problemática se centra exclusivamente en las segundas, que refieren a direcciones temporales asignadas a cada dispositivo cada vez que se conecta a la red.

El tribunal falló indicando que las direcciones IP dinámicas pueden constituir datos personales si hay un proveedor de servicios de internet que pueda conectar la dirección con la identidad de un individuo y si el editor del sitio web tiene medios legales para acceder a la información del proveedor de servicios de internet para identificar al individuo.

El fallo en español puede ubicarse en la siguiente dirección electrónica: http://curia.europa.eu/ con la referencia ECLI:EU:C:2016:779.

Casos "Tele 2, Sverige AB v. Post-och Telestyrelsen" y "Secretary of State for the Home Department v. Watson, Brice, and Lewis"

El 21 de diciembre de 2016 el tribunal falló en los casos "Tele 2, Sverige AB v. Post-och Telestyrelsen" y "Secretary of State for the Home Department v. Watson, Brice, and Lewis", indicando que la ley sueca de Retención de Datos era inconsistente con la Carta Fundamental de Derechos de la Unión Europa.

De esta forma, se confirma la opinión del tribunal respecto de este tipo de retención de información que fuera originalmente establecida en la decisión "Digital Rights Ireland", la cual invalidó la Directiva de Retención de Datos 2006/24/EC y motivó la necesaria adecuación de las legislaciones por gran parte de los países de la Unión Europea.

El fallo llega en un momento en que los gobiernos de la Unión Europea reclaman mayores poderes para sus agencias de seguridad a efectos de investigar ataques terroristas.

En concreto, el tribunal determinó que la conservación de los datos referidos (que incluyen información de emisores y receptores de mensajes de textos e historial de llamadas) permite obtener conclusiones relativas a las vidas privadas de las personas y que las legislaciones nacionales que lo permitan exceden los límites de lo estrictamente necesario, lo que no puede ser justificado en una sociedad democrática.

La retención de información para combatir serios crímenes solo puede ser realizada, según el tribunal, con una previa revisión por un juzgado o cuerpo independiente, excepto casos de urgencia.

El fallo en español puede ubicarse en la siguiente dirección electrónica: http://curia.europa.eu/ con la referencia ECLI:EU:C:2016:970.

06

DIFUSIÓN Y CAPACITACIÓN DE LA URCDP

SITIO WEB

La URCDP ha entendido que la difusión de la información es un elemento sustantivo de su actividad como mecanismo de transmisión del conocimiento del derecho a la protección de datos personales y su garantía.

De esta forma, en 2016 se consideró fundamental continuar con la política de actualización permanente del sitio web, incorporando noticias de interés en la materia y publicando la totalidad de las resoluciones y dictámenes emanados del Consejo Ejecutivo y diferente información que se considera de relevancia.

ATENCIÓN DE CONSULTAS PERSONALIZADAS

La atención de consultas personalizadas, a nivel presencial o telefónico, es una constante del accionar de la unidad.

En ese sentido, se atendieron 490 personas en forma presencial, 685 correos electrónicos y 822 consultas telefónicas, lo que demuestra la continuidad de la penetración y aprehensión del conocimiento vinculado con la existencia y ejercicio del derecho a la protección de datos personales.

Las consultas, con independencia del canal a través del cual se realizan, son variadas y reflejan los diferentes intereses de las personas, los que, en general, se mantienen año a año. Puede establecerse que existe importante interés en los siguientes temas:

- Situación de los expedientes en trámite, sea por consultas o denuncias.
- Inscripción de bases de datos y códigos de conducta.
- Transferencias internacionales de datos.
- Videovigilancia.
- Ejercicio de los derechos de acceso, actualización, supresión o rectificación de datos personales.

CURSO DE PROTECCIÓN DE DATOS EN LÍNEA

En el año 2015, en el sitio web Educantel se colocó a disposición de la ciudadanía el curso en línea de Protección de Datos Personales, que se desarrolló con matrícula libre.

Durante 2016, URCDP y Antel trabajaron conjuntamente a los efectos de promover en la población el conocimiento del Derecho a la Protección de Datos Personales.

El curso continuó facilitando la comprensión de la importancia de la protección de datos personales en la vida diaria, colaborando en la identificación de situaciones en las que se debe tener en cuenta el manejo de los datos personales y las buenas prácticas para protegerlos, así como la comprensión de los conceptos básicos de datos personales y datos sensibles.

Asimismo, el curso explicitó los mecanismos para el ejercicio del derecho, explicándolos de forma concreta y accesible, y las responsabilidades que establece la ley para el manejo de datos personales de otras personas y su adecuado ejercicio a los efectos de su aprehensión por parte de los participantes.

El curso se continuó desarrollando totalmente en línea, siendo sus contenidos presentados de forma amena e interactiva, con interfaces que permiten avanzar y retroceder en los distintos capítulos, así como acceder a breves evaluaciones para que los participantes puedan verificar su grado de aprendizaje.

Además, se incluyeron materiales adicionales disponibles para descargar.

Durante su desarrollo, los participantes han compartido ideas y opiniones con el grupo y han efectuado multiplicidad de consultas a los tutores en el foro de dudas.

En esta segunda edición participaron personas provenientes no solo de Uruguay, sino también de la República del Paraguay.

CHARLAS DE CAFÉ

Las Charlas de Café son una iniciativa de la Unidad Reguladora y de Control de Datos Personales cuyo comienzo como proyecto piloto, durante el último trimestre del año 2015, se extendió exitosamente durante 2016.

Se presentaron como una alternativa para discutir temas de vanguardia desde el foco de la protección de datos personales y el impacto que la inclusión de esta visión en los diferentes ámbitos del quehacer cotidiano verifica.

Las charlas son un mecanismo de acercamiento a propósito de una temática especializada y concreta a los distintos grupos de interés, de forma tal de plantear, a través de expertos especialmente convocados, inquietudes, experiencias, consultas y problemáticas de ineludible análisis.

Así, durante el año 2016 se trabajó a propósito de varios temas que convocaron fuertemente a la reflexión en su vínculo con la protección de datos personales.

"EDUCACIÓN Y PROTECCIÓN DE DATOS"

El 19 de abril comenzó el ciclo Charlas de Café 2016, en donde se abordó el tema "Educación y Protección de Datos".

En calidad de expertos invitados participaron en la instancia la Prof. Alex Mazzei, presidenta del Instituto de Evaluación Educativa, la Dra. María Verónica Pérez Asinari, jefa de la Unidad de Supervisión y Aplicación de la Ley del Supervisor Europeo de Protección de Datos Personales de la Unión Europea, el Lic. Guilherme Canela, coordinador de Comunicación e Información de la Oficina de Unesco en Montevideo, y Felipe Rotondo (moderador), miembro del Consejo Ejecutivo de la URCDP.

Felipe Rotondo estableció que si bien estamos en la era de la sociedad de la información, entre nativos digitales no siempre se toma conciencia de la importancia de alfabetizar digitalmente y de cómo se debe trabajar en la casa y en el aula. Agregó: "La ley dice que el derecho de protección de datos personales es un derecho humano y la educación es clave y puente para los derechos humanos".

Alex Mazzei señaló: "La extensión de los derechos y el uso de las TIC ha cambiado mucho; la introducción de las Ceibalitas en el aula también ayudó a incorporar las TIC. Debemos discutir entre todos, el lugar y el rol que tienen estas herramientas tecnológicas. Son debates que deberían darse en todos los ámbitos".

Por su parte, María Verónica Pérez Asinari indicó: "Sería interesante que las TIC en el aula se enseñen no para meros usuarios, sino de forma activa, a programar, pensar y definir. Sobre todo, el uso de las TIC debe adaptarse a la edad de la persona".

Para Guilherme Canela, "la tecnología está; debemos preguntarnos cómo debemos utilizarla y, sobre todo, qué educación queremos. El mundo entero está pensando en esto. Unesco plantea que debemos hablar de sociedades de conocimiento". También expresó que la tecnología no es un fin en sí mismo, sino "una herramienta en la que vivimos en sociedad y requeriremos de habilidades y aprendizajes". Destacó las TIC como medio, pensar en contenidos y considerar como fin la capacidad de aprender a intervenir y programar, a dominar el contenido, para que el niño y el joven realmente se adueñen de las TIC. Finalizó diciendo: "No se trata de entregar máquinas solamente, sino enseñar a discernir entre qué está bien y qué no. Hoy googleamos todo; ¿cómo sabe un niño qué está bien y qué no?"

Otros de los puntos que se abordaron en la jornada fueron la importancia del sistema educativo como guardián de datos y la forma en que estos se gestionan, la necesidad de contar con protocolos y no permitir que "cada uno haga lo que quiera" para construir un escenario en el que se fortalezca la transparencia y se genere confianza y la posibilidad de incorporar estos temas en las escuelas, no como asignaturas, sino como temas transversales al resto de las materias.

Asimismo, señaló que se debe escuchar más a la población, saber cómo los niños se relacionan con las TIC para diseñar políticas públicas y mejorar las campañas de sensibilización adaptadas a los diferentes destinatarios con ejemplos que estos comprendan.

“IDENTIDAD DIGITAL Y PROTECCIÓN DE DATOS”

La segunda charla del ciclo “Charlas de Café” tuvo como tema de debate la identidad digital y la protección de datos.

El Esc. Gonzalo Sosa, moderador de la mesa, llamó la atención acerca de la cantidad y la calidad de la información que se genera cuando navegamos en internet. Plateando cuál es el concepto de identidad y los desafíos que hay por delante, los expositores participaron muy ávidamente en esta instancia.

Por la Dirección Nacional de Identificación Civil participó el Dr. Ruben Amato, quien precisó la diferencia entre identidad e identificación y manifestó el especial cuidado que se tuvo a la hora de modificar la nueva identificación de los ciudadanos. Asimismo, hizo referencia al concepto de “gobernabilidad democrática”, mencionando que el ser humano necesita identificarse, “saber quién es quién”; el Estado también necesita saberlo para poder cumplir sus funciones y pensar en políticas públicas acordes a su población.

El Esc. Alejandro Santomauro, en su carácter de presidente de la Unidad de Certificación Electrónica, expuso acerca de las garantías que brindan los chips que forman parte de la nueva identificación que imparte la DNIC. Desde la UCE se han generado políticas para que los prestadores se adhieran a ellas, dando así todas las garantías para que el ciudadano pueda relacionarse con el Estado de forma segura. Indicó también que es indispensable “ser conscientes de cómo estamos usando nuestros datos; es una cuestión cultural en la que debemos continuar trabajando”.

También participó el Lic. Roberto Balaguer, en su carácter de especialista en uso de redes sociales. Su disertación radicó en la preocupación de los jóvenes acerca de las estelas que sus intervenciones en las redes sociales han dejado y cómo esta puede afectar su futuro laboral. Subrayó que “las personas se manejan en las redes sociales como si fueran anónimas, pero esto no funciona tan así”. Los chicos con nueve años ya están usando las redes sociales con su propia identidad. Son generaciones “que viven a estadio lleno”, volcando datos casi permanentemente.

Desde la URCDP se indicó que la selección de este tema para incluir en el ciclo de charlas se debió a la necesidad que las sociedades están teniendo para gestionar su identidad digital. En este nuevo mundo en que nos movemos, debemos contar con certezas y seguridades que “posibiliten continuar generando actividad en línea”. Felipe Rotondo manifestó que la Ley de Protección de Datos Personales intenta ser una garantía más frente a este mundo en el que estamos inmersos.

A sala llena y con mucho interés por parte de la audiencia, los expositores debatieron acerca del manejo de estos temas en el marco de las nuevas tecnologías.

"INNOVACIONES TECNOLÓGICAS Y PROTECCIÓN DE DATOS PERSONALES: CIUDADES INTELIGENTES E INTERNET DE LAS COSAS"

La tercera convocatoria del ciclo "Charlas de Café" tuvo como lema: "Innovaciones tecnológicas y protección de datos personales: ciudades inteligentes e internet de las cosas".

En la ocasión participaron la Ing. Cristina Zubillaga, directora de Desarrollo Sostenible e Inteligente de la Intendencia de Montevideo, el Ing. Pablo Brenner, CEO & Founder de Collokia, y el Ing. Miguel Barreto, miembro del Board del Capítulo Uruguay de ISOC y docente de la Facultad de Ingeniería, con la moderación de la Esc. Beatriz Rodríguez Acosta.

Los panelistas pusieron sobre la mesa la discusión acerca de la manera en que las ciudades se preparan y utilizan las tecnologías con la finalidad de prestar servicios de forma eficiente. El disparador inicial fue si los uruguayos estamos dispuestos a dar nuestros datos para acceder a servicios o aplicaciones que tienen en su objetivo facilitarnos la vida.

Barreto indicó que son muchos los "beneficios y riesgos" que hay al respecto y que lo mejor termina siendo "ser cautelosos y no ponernos desnudos frente a las herramientas tecnológicas". Zubillaga, por su parte, reflexionó acerca de la fascinación que provoca la idea de la "automatización de los hogares" y resaltó que podremos resistirnos más o menos, pero a la larga hemos ido adoptando cosas que a priori parecían imposibles, como Facebook o WhatsApp. Brenner resaltó las ventajas que este contexto ofrece a los estudiantes, por ejemplo, los accesos a las distintas bedelías para dar seguimiento a su carrera de forma más eficiente.

¿Qué sucede con las aplicaciones y el pedido de datos para que sean tratados en forma correcta? ¿Por qué las empresas no trabajan en *Privacy by Design*? ¿Qué medidas deberíamos tomar para desarrollar las ciudades inteligentes? Estas fueron algunas de las preguntas sobre las que se debatió y de las cuales surgieron conceptos como "equilibrio", "normativa", "consciencia" y "seguridad". Los panelistas reflexionaron también acerca de la consciencia que los usuarios deberíamos tener sobre el uso de las nuevas tecnologías y qué deberíamos hacer para convertirnos en ciudadanos digitales de verdad, madurando en ese aspecto de la misma manera que evolucionó la tecnología.

Para finalizar, los expositores indicaron que Uruguay posee un marco normativo mucho más claro que años atrás, aunque es tan rápido el avance que no podemos adaptarnos y ya vino otro. En este sentido, se destacó el balance que debemos encontrar y trabajar para disfrutar de los beneficios que las ciudades inteligentes pueden brindar y enfrentar los riesgos que traen aparejadas para adaptarnos con facilidad. Asimismo, se indicó que es necesario incorporar en algunas carreras formación o cursos complementarios que ayuden a profundizar en estos temas que hoy están sobre la mesa.

FILM *DEMOCRACY* Y EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS PERSONALES

En la última instancia del ciclo "Charlas de Café", que tuvo como objetivo reflexionar a propósito del Nuevo Reglamento Europeo de Protección de Datos Personales, participaron el director ejecutivo de Agesic, Ing. José Clastornik, el primer secretario de la Delegación de la Unión Europea en Uruguay, Sr. Tomaz Gorizec, la directora del Goethe-Institut, Dra. Katharina Ochse, y los miembros de la URCDP Ing. Virginia Pardo, Mag. Federico Monteverde y Dr. Felipe Rotondo.

El Dr. Rotondo, en su carácter de presidente de URCDP, indicó que la instancia de compartir una película relevante en la temática de datos personales y poder comentarla con autoridades de la región, así como de la Agencia Española de Protección de Datos y de la Delegación de la Unión Europea en Uruguay, es algo muy especial.

El secretario de la Delegación Europea refirió a la importancia que los datos personales tienen en el mundo; dijo que son "un capital importante" y que su valor aumenta día a día. Por ello, es fundamental acompañar su reglamentación, evitar abusos y trabajar en su prevención. El objetivo principal del nuevo reglamento tiene que ver con los datos personales individuales y la importancia de tomar el control acerca de cómo se los usa y de las obligaciones de quienes manejan y procesan datos. A partir de mayo de 2018, entrará en vigor, luego de un plazo que el reglamento otorga a los actores obligados para que puedan ponerse al día con las nuevas disposiciones. Identificó, a su vez, dos aspectos clave que incorpora el nuevo reglamento: el derecho al olvido y el reforzamiento del procesamiento de datos, previendo multas a quienes no cumplan.

La Dra. Ochse, por otra parte, manifestó que "la democracia necesita demócratas que quieran defenderla y pelear por ella". El Goethe-Institut consiguió los derechos de la película *Democracy. Im rausch der daten* con el objetivo de contribuir al debate público acerca de la importancia de los datos personales. "La globalización ha llegado, pero la manera en que tratamos los datos está intrínsecamente metida en la cultura de cada país", resaltó.

El Ing. Clastornik invitó a los participantes a seguir aportando y contribuyendo a generar una cultura de protección de datos personales. En Uruguay, indicó, hemos tenido grandes avances, pero aún resta mucho por hacer. Estas instancias de trabajo en red, como lo es RIPD a nivel internacional o las Charlas de Café a nivel local, permiten aumentar las competencias y el conocimiento de las personas y organizaciones en relación con el Derecho a la Protección de Datos Personales. Nuestro desafío debe ser avanzar en el empoderamiento ciudadano sobre el ejercicio de este derecho fundamental, así como promover políticas y estrategias en materia de protección de datos personales para la nivelación de las asimetrías entre los países latinoamericanos.

Durante el transcurso de la actividad fue emitida la película Democracia, fiebre de datos (*Democracy. Im rausch der daten*), del director David Bernet.

Todas las instancias contaron con una nutrida asistencia integrada por académicos, autoridades y público en general interesado en estos temas, quienes intercambiaron puntos de vista con los expertos invitados.

CHARLAS IMPARTIDAS EN 2016 A DIFERENTES ENTIDADES

A efectos de continuar avanzando en la aprehensión de conocimiento en la materia por parte de las diferentes entidades y como ya es característico, la Unidad Reguladora y de Control de Datos Personales ha realizado durante todo 2016 una serie de capacitaciones a diversas entidades del Estado y organizaciones sin fines de lucro.

En ese sentido, se llegó con los temas de protección de datos a entidades como la Oficina de Planeamiento y Presupuesto (OPP), el Banco Hipotecario del Uruguay (BHU), el Banco de Previsión Social (BPS), la Administración Nacional de Combustibles, Alcohol y Portland (Ancap), el Centro Ceibal para el Apoyo a la Educación de la Niñez y la Adolescencia (Plan Ceibal), el Programa APEX de la Universidad de la República (APEX) y el Consejo de Educación Inicial y Primaria.

Todos quienes participaron en estas capacitaciones manifestaron su interés en el tema y se mostraron muy activos, presentando sus inquietudes y realizando preguntas al respecto.

Por otra parte, se realizó una charla de capacitación en el evento denominado "Fortalecimiento de la intervención judicial en la protección y promoción del derecho a la libertad de expresión en el Uruguay", organizado por el Centro de Archivos y Acceso a la Información Pública (CAinfo).

REDES DE REPLICACIÓN

Continuando con las actividades vinculadas con las redes de replicación entre las diversas entidades públicas, durante 2016 se continuó trabajando en la capacitación de los portavoces del mensaje relacionado con la importancia de conocer los beneficios de una adecuada protección de los datos personales.

En este sentido, se efectuaron capacitaciones, charlas específicas y charlas de sensibilización dirigidas a las personas designadas como replicadores y al público en general.

07

RELACIONAMIENTO INTERNACIONAL

PRESIDENCIA DE LA RIPD

En noviembre de 2016, durante el Seminario Iberoamericano de Protección de Datos, celebrado en Montevideo, Uruguay asumió la presidencia de la Red Iberoamericana de Protección de Datos Personales, tras la votación realizada en sesión cerrada de los países miembros que la conforman. La presidencia uruguaya comprenderá el período 2017-2019.

La RIPD surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos celebrado en 2003 en La Antigua, Guatemala, con la asistencia de representantes de catorce países iberoamericanos.

Esta iniciativa contó desde sus inicios con un apoyo político reflejado en la Declaración Final de la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos celebrada en Santa Cruz de la Sierra, Bolivia, los días 14 y 15 de noviembre de 2003. Dicha declaración reconoce la protección de datos personales como un derecho fundamental y la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos.

La RIPD se configura así desde sus orígenes como un foro integrador de los diversos actores, tanto del sector público como privado, que desarrollen iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos. Asimismo, busca promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho.

El comité ejecutivo de la RIPD estará integrado, además, por Argentina, Colombia y México; la Secretaría Permanente de la Red es ejercida por la Agencia Española de Protección de Datos, la que asume las tareas de coordinación como órgano técnico y de seguimiento de las actividades de la RIPD.

SIMPOSIO SOBRE CIBERSEGURIDAD Y PRIVACIDAD EN LATINOAMÉRICA Y GLOBAL PRIVACY SUMMIT 2016

Durante el mes de abril, el presidente del Consejo Ejecutivo de la URCDP, Mag. Federico Monteverde, participó en calidad de expositor en dos eventos internacionales.

El 1° de abril participó en el Simposio sobre Ciberseguridad y Privacidad en Latinoamérica, desarrollado en la ciudad de Miami, Estados Unidos, organizado por el estudio internacional de abogados Jones Day. Se discutieron cuestiones de actualidad vinculadas con temas regulatorios en materia de ciberseguridad y privacidad.

Asimismo, entre el 4 y el 6 de abril intervino en el panel de Autoridades de Protección de Datos de América Latina en el marco del evento Global Privacy Summit 2016, organizado por la International Association of Privacy Professionals (IAPP) desarrollado en Washington, Estados Unidos.

Este evento es uno de los más importantes en materia de protección de datos, con más de 4.000 participantes de la industria, el gobierno, la academia y la sociedad civil. En

dicha oportunidad, se realizaron también reuniones con otras autoridades en materia de protección de datos y agencias del gobierno de Estados Unidos.

XIV ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS Y EL IV CONGRESO INTERNACIONAL DE PROTECCIÓN DE DATOS

Entre el 8 y el 10 de junio de 2016 se llevaron a cabo en la ciudad de Santa Marta, Colombia, el XIV Encuentro Iberoamericano de Protección de Datos y el IV Congreso Internacional de Protección de Datos.

El encuentro se dividió en dos instancias. La primera consistió en una sesión cerrada, que tuvo lugar el día 8 de junio por la tarde, en la que miembros, observadores y expertos invitados de la Red Iberoamericana de Protección de Datos se reunieron para debatir a propósito de las últimas tendencias de protección de datos personales. La segunda instancia consistió en una sesión abierta, realizada los días 9 y 10 de junio, conjuntamente con la Superintendencia de Industria y Comercio de Colombia, en el marco de su IV Congreso Internacional de Protección de Datos.

Los temas tratados en el evento fueron divididos en varios paneles, en los cuales diversos expertos hicieron referencia a los cambios en el entorno de la privacidad y la protección de datos personales, el interés legítimo en el tratamiento de los datos personales, seguridad, cooperación entre las autoridades, internet de las cosas y tratamiento de datos personales en las redes sociales, entre otros temas.

En representación de la Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay participó la Esc. María Cecilia Montaña.

IV REUNIÓN DEL COMITÉ AD HOC DE PROTECCIÓN DE DATOS (CAHDATA)

El 15 y el 16 de junio de 2016, en la sede del Consejo de Europa de la ciudad de Estrasburgo, Francia, se llevó a cabo la IV Reunión del Comité Ad Hoc de Protección de Datos (CAHDATA).

El Comité Ad Hoc de Protección de Datos reúne a representantes de los Estados miembros de la Unión Europea integrantes del Consejo de Europa, así como a otros Estados no europeos. El objetivo es proporcionar un foro intergubernamental de alto nivel para negociar, garantizar la coherencia y complementariedad en el marco de la unión y apoyar el potencial global del Convenio Nº 108, de 28 de enero de 2001, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal. Esta norma ha sido internalizada en nuestro ordenamiento jurídico por la Ley Nº 19.030, de 27 de diciembre de 2012.

En el evento se trataron diversos temas, como las reformas proyectadas para la modificación del Convenio Nº 108, así como el examen de las cuestiones pendientes vinculadas con su modernización.

El 17 de junio, con posterioridad a dicha reunión y en el mismo lugar, se llevó a cabo la conferencia internacional denominada "Convenio 108: De una realidad europea a un tratado global". En dicha conferencia se analizó la importancia del Convenio 108 para los países adherentes y su impacto en temas como el comercio, la seguridad y la cooperación internacional. En el caso particular de Uruguay, la URCDP participó en el panel "Adhesión al Convenio 108: beneficios y compromisos", relatando el camino de nuestro país hacia la adhesión al convenio.

Asimismo, en el marco de la conferencia se recibió el instrumento de ratificación del convenio por parte de la República de Mauricio, que se convirtió de esta forma en el 49º país adherente, y se suscribió un acuerdo de cooperación entre las autoridades de Bélgica y Túnez.

En representación de la URCDP participó el Esc. Dr. Gonzalo Sosa Barreto.

33ª REUNIÓN PLENARIA DEL COMITÉ CONSULTIVO DEL CONVENIO Nº 108 DEL CONSEJO DE EUROPA.

Entre los días 29 de junio y 1º de julio se llevó a cabo en la ciudad de Estrasburgo la 33ª Reunión Plenaria del Comité Consultivo del Convenio Nº 108 del Consejo de Europa, del que Uruguay forma parte. El Consejo Ejecutivo de la URCDP estuvo representado por la Dra. Laura Nahabetián Brunet.

En la instancia se trabajó a partir de la presentación del Sr. Filippo Noceda en relación con intercambio de datos en materia tributaria, estableciendo la importancia de la relación entre intercambio de datos y transparencia como elementos para el mantenimiento de la protección de los datos en sí misma y el combate a la corrupción.

Asimismo, se analizó pormenorizadamente el documento de lineamientos desarrollado por el Bureau vinculado con Protección de Datos y Big Data.

Las diferentes delegaciones que oportunamente presentaron comentarios los explicaron y justificaron; el Prof. Alessandro Mantelero destacó como sustantivo que en la medida en que hay varias referencias a una perspectiva ética del Big Data y que los diferentes países en general tienen comisiones de ética, los lineamientos deben analizarse con cierta flexibilidad, ya que las cuestiones éticas y sociales, en alguna medida, responden a las idiosincrasias particulares de cada sociedad.

Se trabajó también sobre el tema de la protección de datos en salud, analizándose el documento vinculado con las recomendaciones para este sector presentado por el Bureau, lo que se realizó bajo la dirección de Jeanne Bosse Malatosse.

Bajo la dirección de Marie George se analizó el documento de recomendaciones denominado Passengers Name Records y con la dirección de Bertil Cottier se consideró el documento vinculado con Protección de Datos y medios de comunicación, particularmente, en su relación con los periodistas.

Finalmente, se procedió a la votación para la integración del nuevo Comité del TP-D, que quedó integrado por Italia (presidente), Suiza (primer vicepresidente), Luxemburgo (segundo vicepresidente), Georgia, Servia, Portugal, Francia y Hungría.

38ª CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Desde hace 38 años, las autoridades de Protección de Datos Personales se reúnen cada año en diversos lugares del mundo en la Conferencia Internacional de Privacidad. En 2016, lo hicieron en la ciudad de Marrakech, Marruecos, entre el 17 y el 20 de octubre.

En representación de la Unidad Reguladora y de Control de Datos Personales participó el presidente del Consejo Ejecutivo, Dr. Felipe Rotondo.

La conferencia constó de dos partes: una sesión cerrada para las autoridades y una sesión abierta a todo público.

En la sesión cerrada se trató una nutrida agenda en la que se expusieron temas tales como robótica, inteligencia artificial, encriptación, acceso autorizado a comunicaciones encriptadas y privacidad en la era digital; y en la sesión abierta a todo público se desarrollaron temas como privacidad y protección de datos como motor de desarrollo sostenible, adecuación, localización y determinismo cultural, tendencias de las tecnologías y la privacidad.

También se reflexionó a propósito de qué impacto tienen estos temas sobre la privacidad, cómo conciliar la seguridad y la privacidad y los desafíos de la educación digital.

SEMINARIO "DERECHO AL OLVIDO, TUTELA INTEGRAL DE LA PRIVACIDAD. VISIÓN IBEROAMERICANA"

El 23 de agosto, el presidente del Consejo Ejecutivo de URCDP, Dr. Felipe Rotondo Tornaría, participó en la ciudad de México en el seminario "Derecho al olvido, tutela integral de la privacidad. Visión Iberoamericana", organizado por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Inai).

El objetivo del evento fue analizar el derecho al olvido en el marco de la salvaguarda de los datos personales, sus diferentes dimensiones, los criterios jurisprudenciales en Iberoamérica y las soluciones alternativas.

El Dr. Rotondo participó en el panel denominado "Las dimensiones del derecho al olvido", en el que se analizaron las vertientes patrimonial, política, judicial, víctimas y laboral.

En el panel estuvieron también presentes Guillermo Antonio Tenorio, profesor de la Universidad Panamericana y director del Centro de Estudios del TFJF, Olivia Mendoza, investigadora de Infotec, y Ma. Patricia Kurczyn, comisionada del Inai.

Además, se trataron temas como "El derecho al olvido", "Fórmula de protección de la privacidad y los datos personales" y "La experiencia de la tutela jurisdiccional en Chile, Colombia y México".

FORO DE AUTORIDADES DE PRIVACIDAD DE ASIA PACÍFICO (APPA)

Durante la semana comprendida entre el 30 de noviembre y el 2 de diciembre se realizó en Manzanillo, Estado de Colima, México, el Foro de Autoridades de Privacidad de Asia Pacífico (APPA).

Este foro contó con una reunión abierta y una reunión cerrada; en ambas participó la Unidad Reguladora y de Control de Datos Personales (URCDP) en la categoría de observador, junto con la Agencia Española de Protección de Datos, el Grupo de la Francofonía y el Ministerio del Interior de Corea.

En la reunión abierta se trataron temas como transferencias internacionales de datos, cooperación internacional, autorregulación y resolución de controversias. La reunión cerrada tuvo como centro temas relativos al Foro de Autoridades de Privacidad de Asia Pacífico y la última Conferencia Internacional de Autoridades de Privacidad y Protección de Datos que tuvo lugar en Marruecos.

En este foro participaron autoridades de Australia, Canadá, Columbia Británica, Colombia, Corea, Estados Unidos, Hong Kong, Japón, Macao, México, Nueva Gales del Sur, Nueva Zelanda, Perú y Singapur.

Por la Unidad Reguladora y de Control de Datos Personales participó la Dra. Beatriz Rodríguez Acosta en el panel "Global privacy updates and developments". Durante su exposición compartió la experiencia uruguaya en materia de relacionamiento internacional y el espíritu de colaboración y cooperación que se pretende entablar con otras redes

de la región. Asimismo, en representación del país que preside la Red Iberoamericana de Protección de Datos Personales (RIPD), la Dra. Rodríguez detalló los lineamientos que se seguirán en base al Documento Estratégico RIPD 2020.

ENCUENTRO CON REFERENTES ACADÉMICOS Y AUTORIDADES DE PROTECCIÓN DE DATOS

Visita del Dr. Juan Antonio Travieso

El 9 de marzo, el Dr. Juan Antonio Travieso visitó la URCDP. Se trata de un reconocido profesor universitario y especialista en materia de protección de datos personales. Fue quien impulsó las actividades institucionales en materia de protección de datos personales en la República Argentina, transformando durante su mandato la Dirección Nacional de Protección de Datos Personales en una entidad de referencia en América Latina.

Además, durante su período Uruguay inició sus actividades en la materia y él colaboró en la trasmisión de conocimiento teórico y práctico con miras a la implementación efectiva de este derecho en el país.

Oportunamente, se realizaron intercambios fructíferos entre ambos países y estas instancias permitieron compartir experiencias y lecciones aprendidas.

Esta visita permitió a los equipos jurídicos de Agesic y a los miembros de los círculos académicos cercanos a la URCDP continuar intercambiando ideas en esta materia con un especialista reconocido que ha sido, además, un colaborador de la URCDP desde sus inicios.

Visita de la Dra. María Verónica Pérez Asinari

El 19 y 20 de abril visitó la URCDP la Dra. Mª Verónica Pérez Asinari, jefa de la Unidad de Supervisión y Aplicación de la Ley del Supervisor Europeo de Protección de Datos.

La profesional visitó el país en el marco de una gira que realiza por las unidades de Protección de Datos de Argentina y Uruguay. Compartió sus conocimientos en relación con los roles del Supervisor Europeo de Protección de Datos y el nuevo reglamento europeo de protección de datos. También realizó un intercambio en relación con la práctica y las tendencias en materia de supervisión de datos personales con miembros del equipo profesional de la unidad.

Además, sostuvo un interesante intercambio en la URCDP con miembros del equipo de Derechos Ciudadanos de Agesic y académicos de la Facultad de Derecho de la Udelar. En esa instancia informó sobre su rol en el Supervisor Europeo de Protección de Datos, sobre cómo este está implementando el vínculo y la colaboración con las autoridades de Protección de Datos Personales, sobre la reforma legislativa de la Unión Europea a través

del Reglamento General de Protección de Datos que sustituye a la Directiva 95/46/CE, su implementación en un plazo de dos años para los países de la Unión Europea y cómo influirá en los terceros países con declaración de adecuación.

Visita del Dr. Pablo Palazzi

El 17 de junio, la Unidad Reguladora y de Control de Datos Personales (URCDP) recibió la visita del Dr. Pablo Palazzi, abogado, profesor, director del Centro de Tecnología y Sociedad de la Universidad San Andrés de la ciudad de Buenos Aires, República Argentina, y editor e integrante del Comité Académico Internacional de la Revista Latinoamericana de Protección de Datos Personales.

En su disertación, el Dr. Palazzi hizo énfasis en el proyecto de reforma de la Ley de Protección de Datos de su país, que fuera presentado por el nuevo director nacional de Protección de Datos de Argentina, Dr. Eduardo Bertoni.

Con el proyecto se espera concretar la modernización de la ley y adaptarla a los nuevos lineamientos del Reglamento General de Protección de Datos, aprobado recientemente por la Unión Europea.

A su vez, este proyecto fue puesto a disposición de la población mediante consulta pública a efectos de que la ciudadanía argentina aportara sus comentarios al respecto.

La disertación del Dr. Pablo Palazzi fue presenciada por representantes del Consejo Ejecutivo y del Consejo Consultivo de la URCDP, así como por miembros de Agesic y la academia.

Visita de miembros del Instituto de Acceso a la Información Pública de la República de El Salvador

El 10 de noviembre se realizó una reunión entre miembros de la URCDP y del Instituto de Acceso a la Información Pública de la República de El Salvador.

La reunión contó con la presencia del comisionado del Instituto de Acceso a la Información Pública, Dr. Jaime Campos, el coordinador de Protección de Datos, Dr. Carlos Calderón, y el magistrado propietario del Tribunal Superior Electoral, Dr. Fernando Argüello Téllez.

Se analizaron diversos temas relativos a la protección de datos personales, la formas de colaboración y cooperación que puedan surgir entre ambas autoridades y los criterios adoptados en cada uno de los temas.

En la instancia, se acordó avanzar en intercambios que lleven a afianzar los vínculos entre ambas autoridades a nivel de gestión y cooperación.

08

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

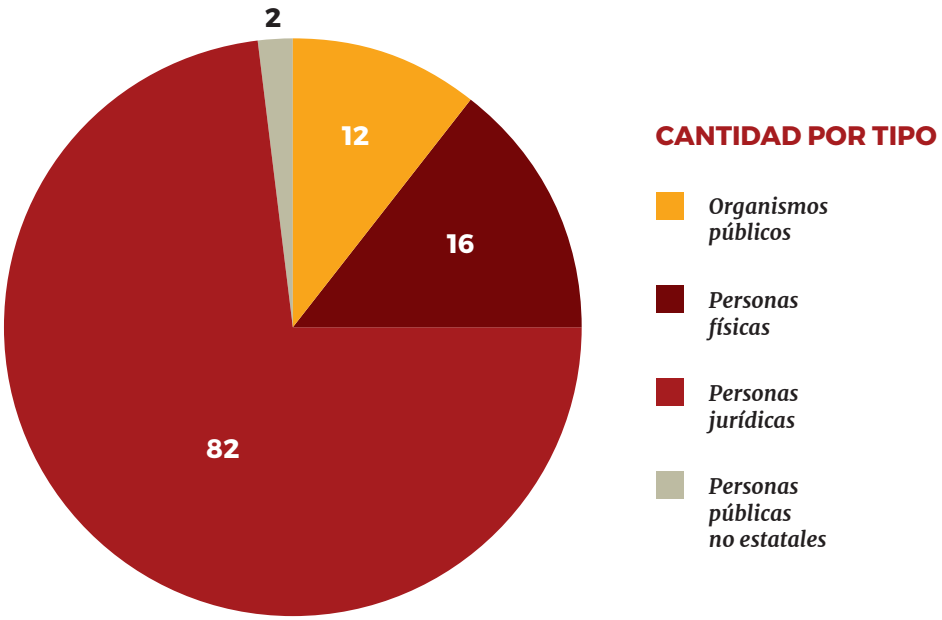
En abril de 2016 se puso a disposición de los responsables de Bases de Datos un nuevo sistema totalmente informatizado que permite el envío y formalización de todos los procedimientos necesarios para la inscripción definitiva de las bases en el registro que lleva adelante la unidad.

De esta forma, se continúa con el proceso de brindar herramientas que faciliten el cumplimiento de las obligaciones impuestas por la ley, a la vez que se procura posicionar al Registro de Bases de Datos de Uruguay a la vanguardia de los sistemas de registro.

En las tablas y gráficos siguientes se presentan los resultados del registro online de los formularios presentados y aprobados durante el año 2016.

Se presentan, en primer lugar, los datos de cantidad de responsables discriminados por tipo, distinguiendo entre entidades públicas, personas físicas, personas jurídicas y personas públicas no estatales.

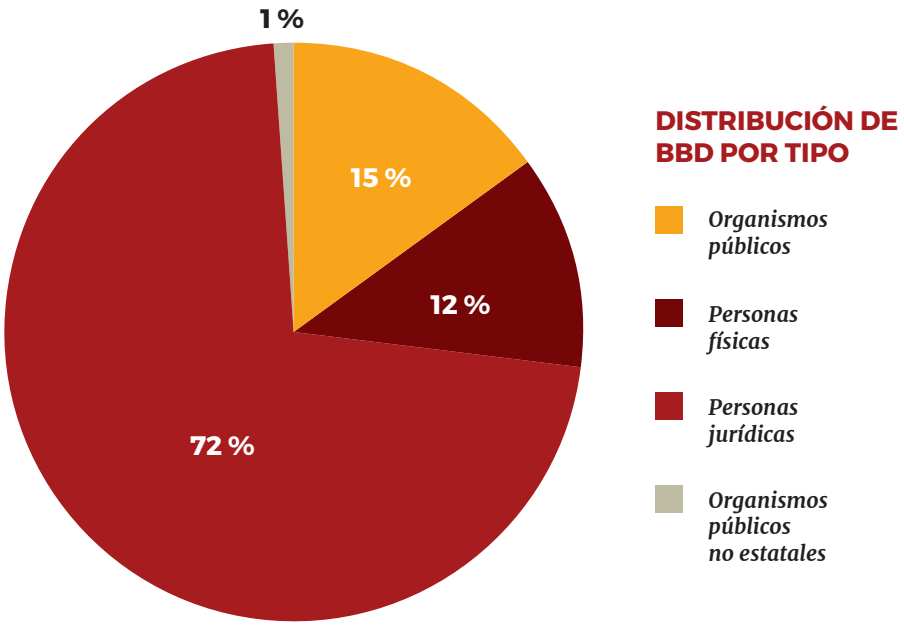
Tipo de responsable	Cantidad
Organismos públicos	12
Personas físicas	16
Personas jurídicas	82
Personas públicas no estatales	2

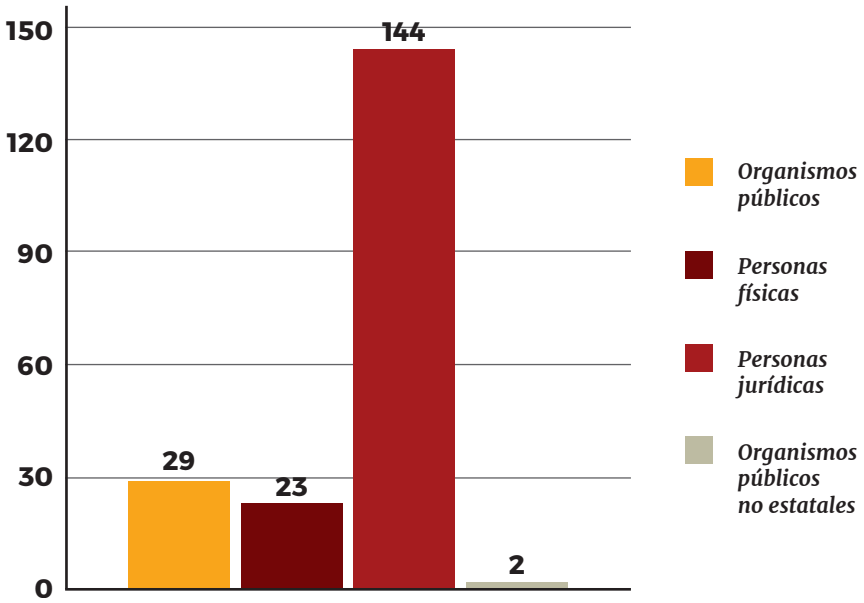


Se observa, al igual que en años anteriores, una mayor tendencia al cumplimiento de las personas jurídicas con respecto a las personas físicas. En el caso de los organismos públicos y las personas públicas no estatales, no han existido variaciones en las tendencias observadas en años anteriores.

Se presentan, a continuación, los datos de cantidad de bases de datos inscriptas en 2016, discriminadas por tipo de responsables.

Tipo de responsable	Porcentaje en total
Organismos públicos	15%
Personas físicas	12%
Personas jurídicas	72%
Personas públicas no estatales	1%





Se observa que en el último año se mantiene la inscripción de bases de datos por parte de personas físicas, organismos públicos y personas públicas no estatales con respecto a la cantidad de inscripciones realizadas por personas jurídicas.

Independientemente de ello, continúa siendo superior la cantidad de bases de datos inscriptas por personas jurídicas con respecto a los demás tipos de responsables.

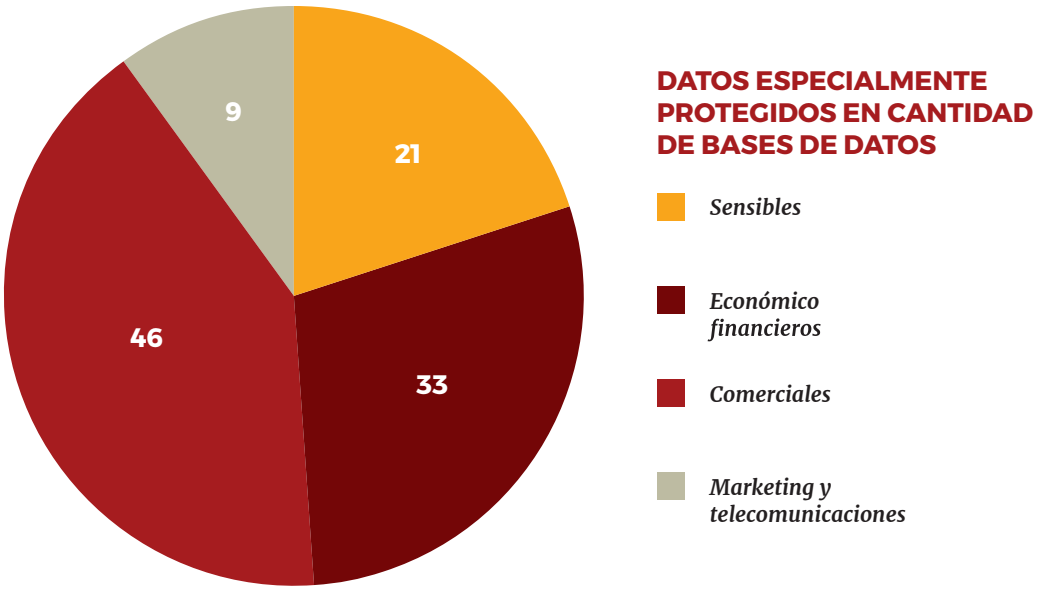
Debe tenerse presente que las resoluciones de inscripción de las bases de datos se dictan por cada responsable, con independencia del número de bases que cada uno de ellos procure inscribir ante el registro que lleva adelante esta unidad.

DATOS ESPECIALMENTE PROTEGIDOS

La consideración de determinados datos como especialmente protegidos por la ley hace necesario un grado especial de cuidados no solo por parte de los responsables de las bases de datos, sino también por parte del organismo de contralor al momento de evaluar los mecanismos de seguridad implementados por los primeros.

Dentro de los datos especialmente protegidos, la ley hace referencia a datos sensibles, datos relativos a la salud, datos relativos a telecomunicaciones, datos relativos a bases con fines de publicidad y datos relativos a la actividad comercial o crediticia.

Conocer la cantidad de bases de datos que contienen este tipo de información es de especial relevancia, habiéndose instaurado un nuevo mecanismo de clasificación de las bases, siguiendo los lineamientos de la ley, con la puesta en línea del nuevo sistema de registro. Con respecto a las bases enviadas por el nuevo sistema, cabe distinguir entonces:



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 el año 2016 se declararon transferencias internacionales en un 10% de las bases de datos.

El hecho de que los países a los que se realizan dichas transferencias cuenten con niveles adecuados de protección en la materia resulta de especial relevancia, en virtud de la existencia de diferentes tipos de requisitos para unas y otras.

Resulta relevante recordar que Uruguay es uno de los pocos países de América que desde el año 2012 fueron declarados por la Comisión Europea adecuados para la realización de transferencias internacionales, ya que cuenta con una regulación de protección de datos acorde a los estándares europeos.

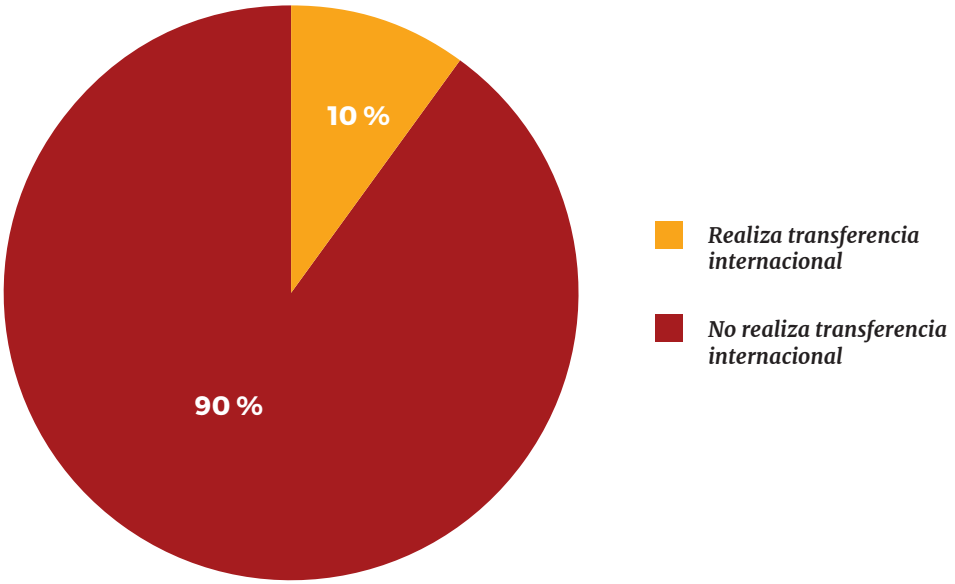
Asimismo, corresponde señalar que luego de la invalidez determinada por la sentencia del Tribunal de Justicia Europeo vinculada al *Safe Harbor*, el régimen de transferencias a Estados Unidos de América fue modificado sustancialmente.

Como se mencionó en capítulos anteriores, 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 residentes en la Unión Europea ante transferencias a los Estados Unidos de América. Conforme lo indica la propia Comisión Europea en http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm, el nuevo acuerdo incluye:

- Fuertes obligaciones de protección de datos para empresas que reciban datos personales desde la Unión Europea.
- Salvaguardas para el acceso del gobierno de Estados Unidos a los datos.
- Protección efectiva y compensaciones para los individuos.
- Revisión anual conjunta para monitorear la implementación.

Este marco de protección se entiende aplicable a las transferencias internacionales que se realicen por responsables de bases de datos de nuestro país a los Estados Unidos, conforme lo establecido en la resolución del Consejo Ejecutivo Nº 17/009, de 12 de junio de 2009.

En 2016 se declararon transferencias internacionales a 53 países, además de aquellas realizadas a la Unión Europea. Resultaron notoriamente superiores las transferencias realizadas a países considerados adecuados, además de Estados Unidos y Canadá.



El mayor volumen de datos se muestra en la tabla siguiente y determina el listado de países a los que se declaró el mayor número de transferencias internacionales de datos:

Puesto	País
1	Estados Unidos de América
2	República Argentina
3	Unión Europea

TIPO DE INFORMACIÓN SEGÚN SU FINALIDAD

Toda base de datos debe ajustarse a una finalidad determinada, la cual no solo debe informarse a los titulares de los datos sino que, además, cumple un rol preponderante a la hora de realizar el tratamiento de la información contenida en ella. Este elemento, en consecuencia, es uno de los más relevantes al momento de la inscripción.

Con respecto a la información contenida, puede señalarse que, al igual que en años anteriores, la gran mayoría de las bases de datos integran datos de carácter identificativo y personal.

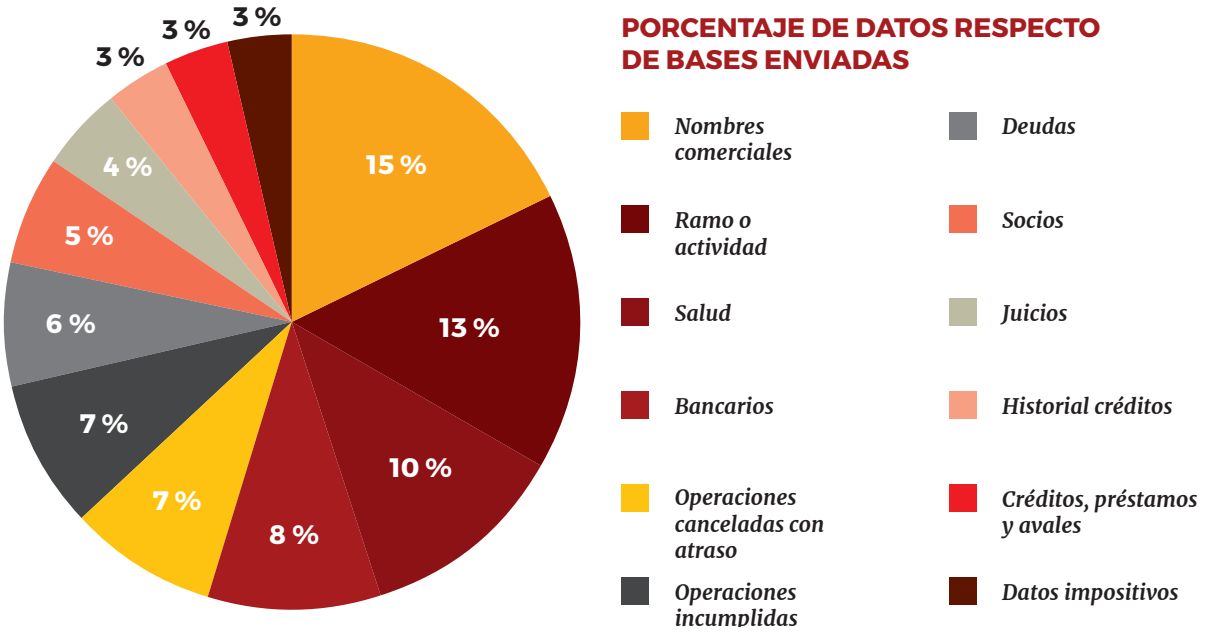
Buena parte de esas bases contienen información que ingresa dentro de la categoría de "datos especialmente protegidos", de acuerdo con la normativa nacional vigente.

Los datos especialmente protegidos son:

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

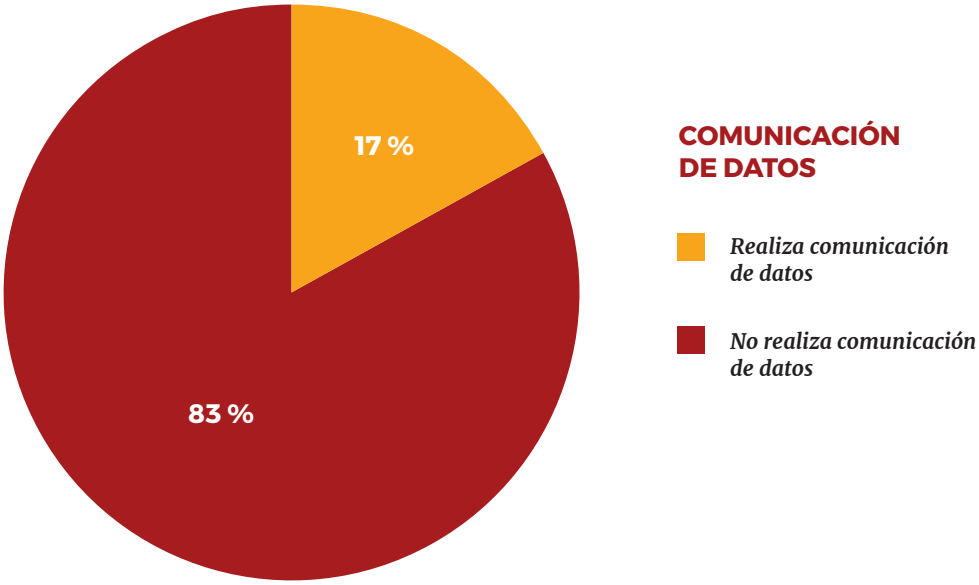
En el listado siguiente se muestran los porcentajes de tipos de datos almacenados y tratados en las bases de datos inscriptas en 2016, conforme la información ingresada en los correspondientes formularios de inscripción y considerando el tipo de información sobre la cantidad de bases enviadas por el nuevo sistema:

Tipos de datos	Porcentaje
Nombres comerciales	15%
Ramo o actividad	13%
Salud	10%
Bancarios	8%
Operaciones canceladas con atraso	7%
Operaciones incumplidas	7%
Deudas	6%
Socios	5%
Juicios	4%
Historial de créditos	3%
Créditos, préstamos y avales	3%
Datos impositivos	3%



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 el año 2016 ascienden a un 17%.



Pueden distinguirse las comunicaciones de datos en gratuitas y onerosas; en el año 2016 todas las declaradas han sido gratuitas.

TIPO DE SOPORTE DE REGISTRO DE BASE DE DATOS

Los soportes utilizados para las bases de datos registradas son:

- Manual.
- Informatizado.
- Manual e informatizado (mixto).
- Otros.

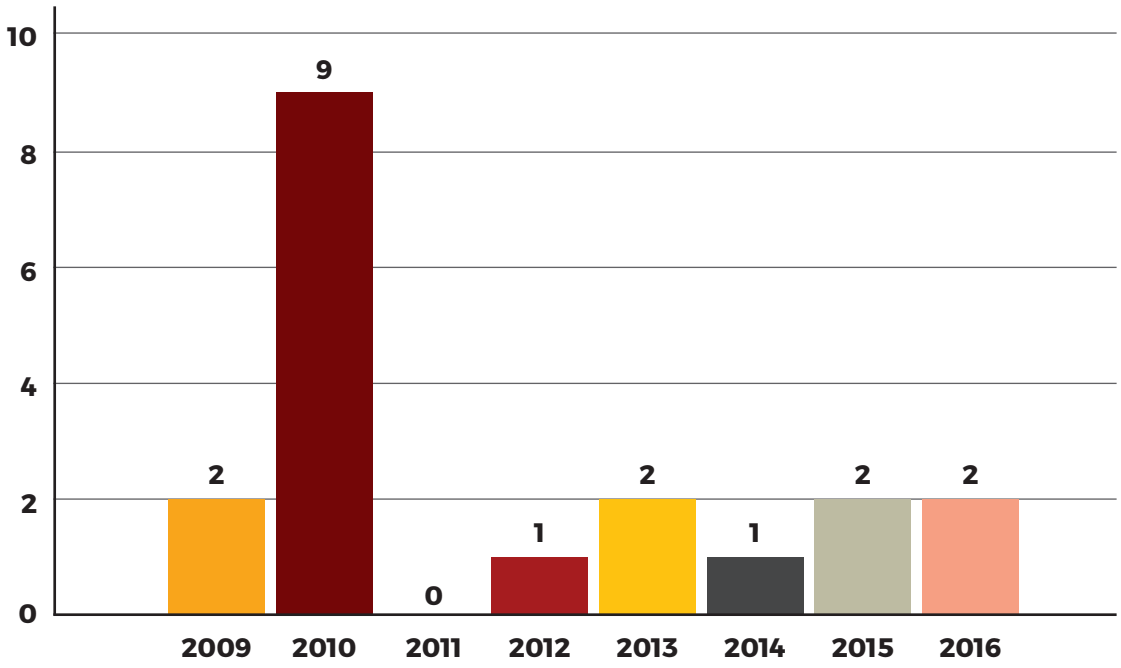
CÓDIGOS DE CONDUCTA

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 2016 se aprobaron dos códigos de conducta.

El análisis comparado de la inscripción de códigos de conducta ante la URCDP se muestra en el gráfico siguiente:

CANTIDAD DE CÓDIGOS DE CONDUCTA POR AÑO



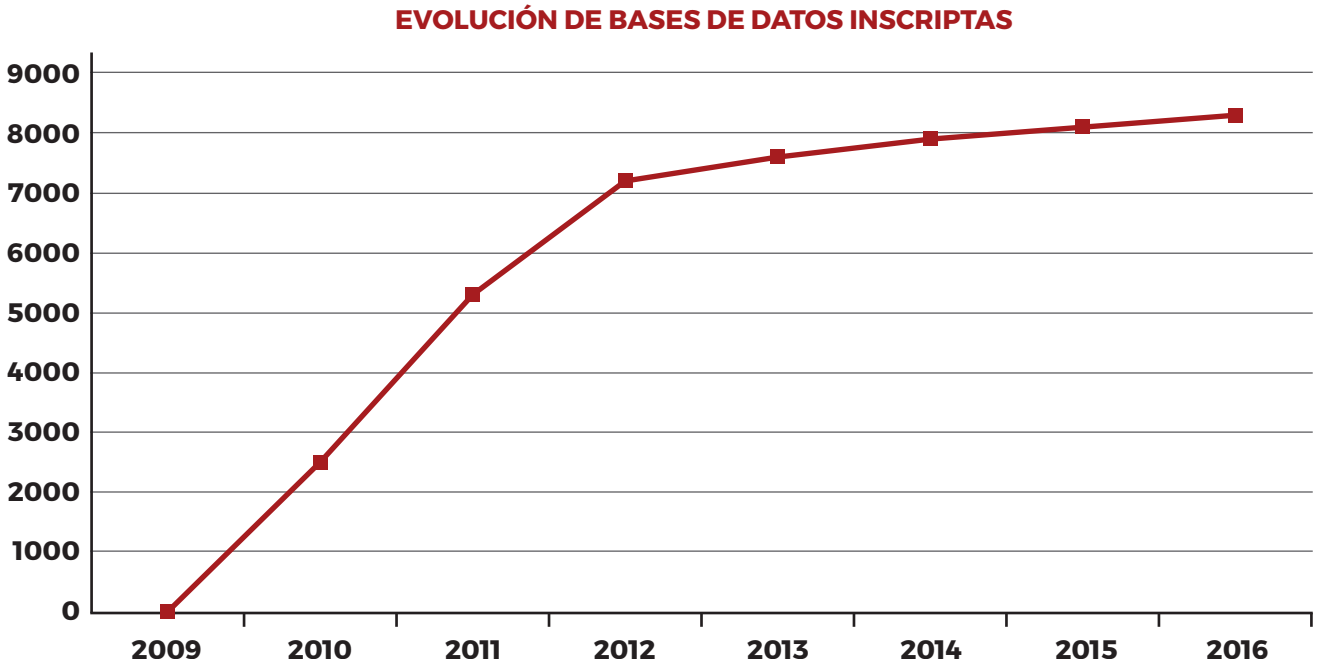
BASES DE DATOS INSCRIPTAS ANTE LA URCDP

Con la implantación del nuevo sistema de registro, el proceso de análisis y aprobación de bases de datos se ha visto notoriamente simplificado. No obstante, en líneas generales puede afirmarse que se mantienen tres valoraciones.

- 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 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 electrónica avanzada de la unidad.

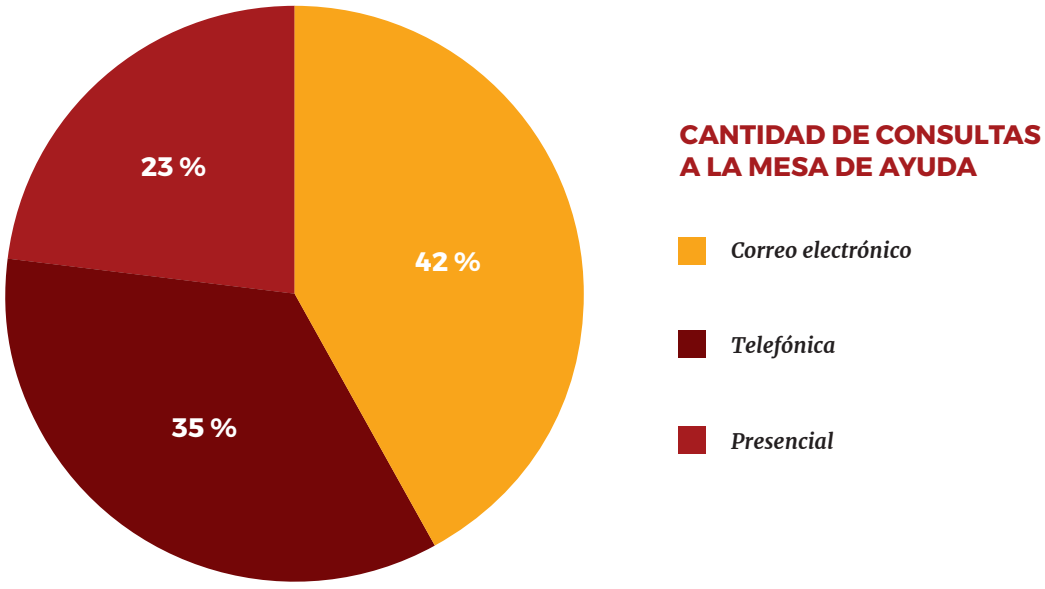
El siguiente gráfico muestra la evolución anual de bases de datos inscriptas.



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 de la división Derechos Ciudadanos de Agesic.

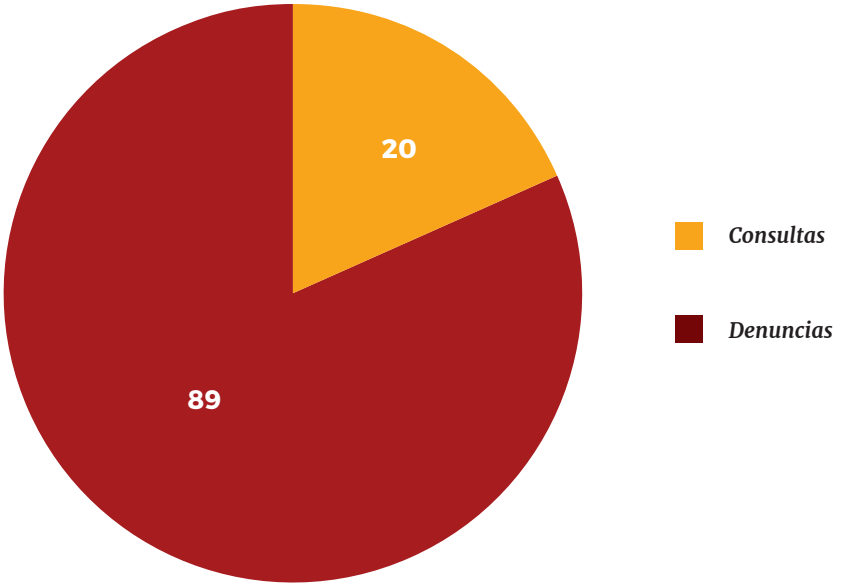
Del total de las consultas que se recibieron durante 2016, 23% se realizaron por la vía presencial, 35% telefónicas y 42% a través del correo electrónico y el formulario de contacto. Ello se muestra en la gráfica siguiente:



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 2016, la URCDP recibió 20 consultas y 89 denuncias, respecto de las cuales se formalizó expediente.



RESOLUCIONES QUE IMPONEN SANCIONES

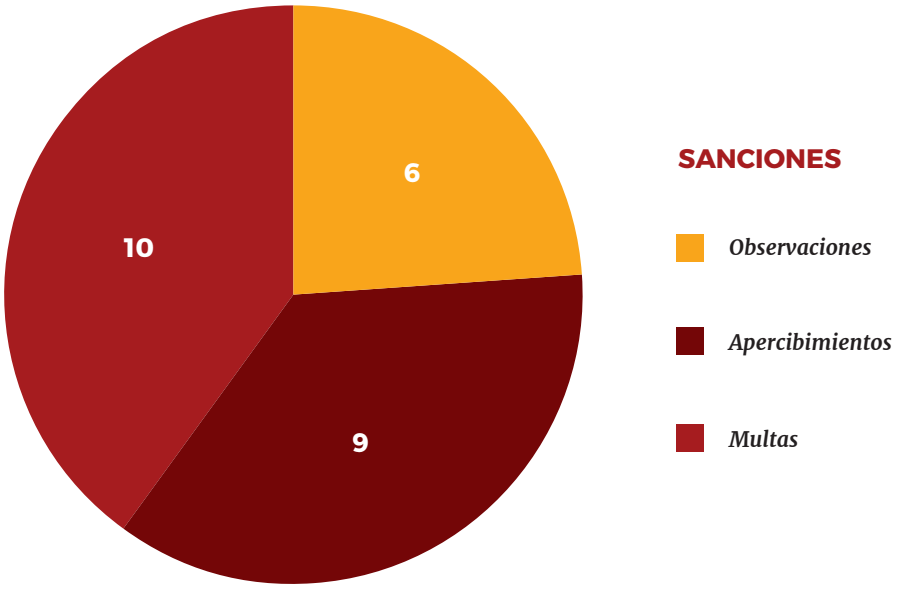
La URCDP tiene competencias en materia de determinación de sanciones otorgadas por el artículo 35 de la Ley Nº 18.331, en la redacción dada por el artículo 152 de la Ley Nº 18.719, de 27 de diciembre de 2010.

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, modificando la escala de sanciones a fin de adecuarla a las actuales tendencias sancionatorias y considerando la importancia de educar a los responsables y encargados de tratamiento.

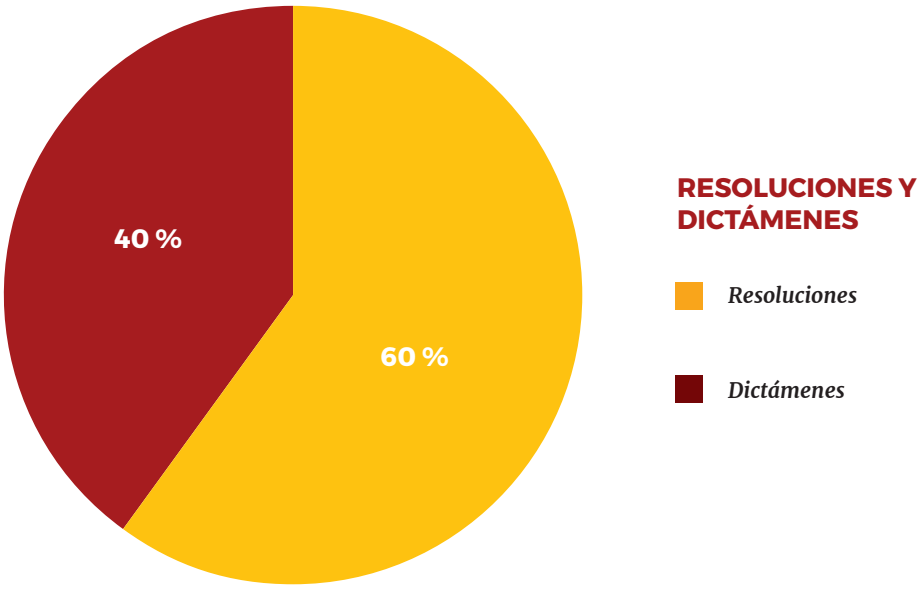
Durante 2016, se aplicaron 6 observaciones, 9 apercibimientos y 10 multas.



RESOLUCIONES Y DICTÁMENES REALIZADOS EN 2016

Durante 2016 se analizaron los expedientes presentados ante la URCDP y se constató la expedición de 34 resoluciones y 23 dictámenes vinculados a expedientes de denuncias y consultas tramitadas ante esta unidad.

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



CANTIDAD DE INFORMES REALIZADOS

En función de los requerimientos que ha recibido la URCDP, se han elaborado 287 informes, que incluyen los puntos de vista jurídico, notarial y técnico referidos anteriormente.

09

LA URCDP ANTE LOS NUEVOS RETOS EN MATERIA DE PROTECCIÓN DE DATOS

A efectos de avanzar en los desafíos presentes y futuros que el derecho a la protección de datos personales presenta, la Unidad Reguladora y de Control de Datos Personales se ha planteado avanzar en acciones partiendo, particularmente, de un análisis estratégico en cuatro ejes, a saber:

PROMOCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS

Bajo este eje se prevén actividades de sensibilización y capacitación con el objetivo de brindar conocimientos acerca del derecho a la protección de datos personales, así como sus mecanismos de ejercicio y protección.

Una de las grandes líneas de trabajo de la URCDP se relaciona con las actividades de sensibilización y capacitación en lo que respecta al conocimiento de la existencia del derecho a la protección de datos personales, procurando mejorar los porcentajes de conocimiento que sobre este derecho manifiestan tener las personas.

Es así que en 2017 está previsto realizar una serie de acciones que procuran aumentar la cantidad de personas que poseen conocimientos sobre la existencia del derecho a la protección de datos personales, así como sus mecanismos de ejercicio y protección.

Actividades previstas para 2017

- Nueva edición del concurso infantil de la campaña "Tus Datos Valen". Se trata de un concurso dirigido a estudiantes de 5º y 6º años de escuelas públicas y privadas del país, quienes a partir de una determinada consigna deberán resolver situaciones problemáticas que involucren datos personales. Será el quinto año consecutivo en que se desarrolla esta actividad.

GOBERNANZA Y FORTALECIMIENTO DE CAPACIDADES

Bajo este eje se consideran acciones vinculadas con el objetivo de brindar herramientas que permitan a los ciudadanos ejercer su derecho a la protección de datos personales, así como incrementar la masa crítica vinculada con la temática.

La URCDP ha incorporado entre sus acciones estratégicas aquella vinculada con la entrega a las personas de las herramientas imprescindibles para el ejercicio de su derecho a la protección de datos personales, con independencia del ámbito de actuación que a cada uno le corresponda. Asimismo, tiene entre sus objetivos facilitar el intercambio entre funcionarios públicos y operadores privados vinculados con el tema y analizar y elaborar propuestas de desarrollo a partir de buenas prácticas nacionales e internacionales.

La URCDP se ha propuesto incrementar en 2017 la masa crítica relacionada con el derecho a la protección de datos personales y su conocimiento para la generación de instancias de discusión tendientes a la evolución de los marcos regulatorios nacionales en la materia.

Actividades previstas para 2017

- Desarrollo de instancias de capacitación. Se realizarán diferentes instancias en entidades públicas y privadas de Montevideo y el interior del país con distintos niveles de profundidad y especificidad, de acuerdo con los requerimientos de los interlocutores para focalizar en necesidades específicas.

- Elaboración de guías y marcos de referencia. Estos documentos se desarrollarán bajo la modalidad de consejos e indicaciones a propósito de los lineamientos fundamentales que se deben tener en cuenta frente a diferentes situaciones.
- Avanzar en la privacidad desde el diseño. Se diseñarán, planificarán y desarrollarán guías e instancias de capacitación vinculadas específicamente con el tema de la privacidad desde el diseño. Particularmente, estas actividades se realizarán en el marco de las actividades que se instrumentan conjuntamente con el ICT4V.
- Segunda Semana Nacional de la Protección de Datos. Se llevará a cabo una nueva Semana Nacional de Protección de Datos Personales, como una forma de reunir a referentes nacionales e internacionales en los diferentes temas y articular la discusión con todos quienes trabajan en la materia o se sienten interesados en aumentar sus conocimientos.

FORTALECIMIENTO Y POSICIONAMIENTO DE LA UNIDAD

El objetivo de este eje es consolidar a la unidad como un referente a nivel nacional en lo que respecta a la protección de datos personales y fomentar la discusión en torno al tema de acuerdo con las modificaciones normativas a nivel internacional.

Institucionalmente, se ha establecido que la URCDP es el ente regulador en todo lo referente a la protección de datos personales, por lo que se le atribuyeron funciones y competencias en ese sentido. Posicionar fuertemente esas competencias, darlas a conocer entre las personas y proteger el derecho a la protección de datos personales son algunos de los objetivos sustantivos de la unidad en su condición de garante del respeto de este derecho fundamental.

En tal sentido, está previsto que en 2017 la URCDP continúe trabajando para consolidarse como un referente nacional en materia de protección de datos personales, no solo en lo que respecta a la regulación del derecho positivo vigente, sino también en lo que refiere a la aprehensión por parte de la población. Fomentar la discusión en torno a esta temática, en virtud de las importantes modificaciones normativas que se han verificado a nivel internacional y el surgimiento permanente de nueva tecnología que interpela a la protección de datos y sus garantes, es una de las tareas inherentes a la unidad desde el momento de su creación.

Actividades previstas para 2017

- Evolución del marco normativo. A efectos de evaluar las disposiciones normativas existentes a la luz de los avances jurídicos y tecnológicos nacionales y extranjeros, se considerará el derecho nacional vigente para determinar la necesidad de sugerir los ajustes e incorporaciones que se entiendan pertinentes.
- Desarrollo del Primer Texto Ordenado de Protección de Datos Personales. Conocer el derecho vigente es importante para todas las personas, motivo por el cual se pretende poner a disposición la normativa en materia de protección de datos personales en forma actualizada y concatenada para una mejor comprensión y ejercicio de este derecho.
- Segunda edición de la Revista Uruguaya de Protección de Datos Personales. El conocimiento de la doctrina, la jurisprudencia y el derecho positivo vigente es central para el ejercicio de ciudadanías activas; por tanto, en 2017 será publicada

una nueva edición de la revista que contiene toda esta documentación, a efectos de facilitar el conocimiento de las tendencias y opiniones de profesionales y autoridades de vanguardia en la materia.

- Continuación del ciclo Charlas de Café. El vínculo entre las TIC y el derecho a la protección de datos personales es muy importante, por lo que se ha entendido interesante realizar un ciclo de charlas para debatir acerca de las diferentes tecnologías que han hecho irrupción en la sociedad con foco en protección de datos personales. En 2017 se continuará por ese camino, iniciado exitosamente en 2015.

RELACIONAMIENTO INTERNACIONAL

Dentro de sus objetivos estratégicos para 2017, la URCDP ha previsto desarrollar relaciones de cooperación con autoridades y expertos en la materia pertenecientes a los cinco continentes, en el entendido que la construcción y el ejercicio efectivo de este derecho revisten carácter colectivo.

Es así que la URCDP seguirá fortaleciendo las redes de intercambio que se han desarrollado hasta la fecha y colaborando en la consolidación de la Red Iberoamericana de Protección de Datos Personales (RIPD) como referente iberoamericano en la materia.

Actividades previstas para 2017

- Participación en la RIPD. Uruguay tiene a su cargo la presidencia de la Red Iberoamericana de Protección de Datos. En el ejercicio de dicha función, se planteará el plan de trabajo a desarrollar en el bienio y avances para su aprobación, el cual es una especificación del Documento Estratégico RIPD 2020.
- Participación en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. La URCDP participará en la conferencia que tendrá lugar en Hong Kong. Esta conferencia reúne anualmente a las autoridades de protección de datos y privacidad de todo el mundo, con el propósito de discutir temas de vanguardia en vínculo directo con la protección de datos personales.
- Participación en las reuniones plenarias vinculadas con el Convenio Nº 108 de Protección de Datos Personales. Además de esta participación, la URCDP realizará en forma constante aportes a los documentos de trabajo remitidos. Se trata de instancias derivadas de la ratificación por Uruguay del Convenio Nº 108, a partir de las cuales se desarrollan lineamientos de política vinculados con protección de datos personales, documentos de trabajo y análisis de expertos y autoridades en la materia.
- Participación en ámbitos temáticos. URCDP participará en foros presenciales y virtuales vinculados con la temática de protección de datos personales en diferentes partes del mundo y con profesionales, académicos y autoridades de los cinco continentes para el intercambio de conocimientos y experiencias.

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES